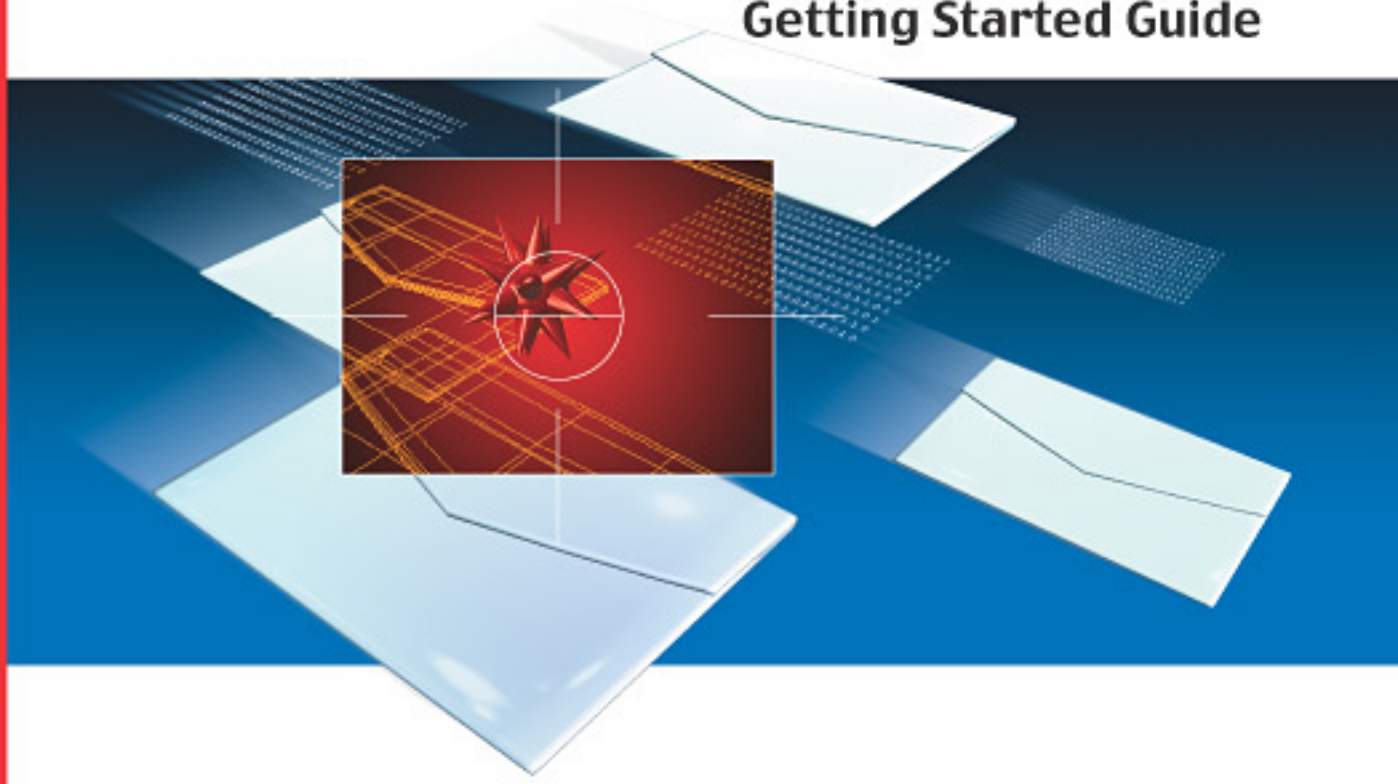
TREND MICRO™

ScanMail™ 2

Keeps viruses out of your Lotus Notes environment

for Lotus. Notes

Getting Started Guide



TREND MICRO™

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

http://www.trendmicro.com/download/default.asp

NOTE: A license to the Trend Micro Software includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

http://www.trendmicro.com/en/purchase/license/license.htm

ScanMail, ServerProtect, InterScan, VirusWall, MacroTrap, TrendLabs, Trend Micro, Trend Micro Incorporated, and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in certain jurisdictions. All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright © 1997-2004 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. SNEM20902/11115

Release Date: April 2003, last updated 1/26/04

Protected by U.S. Patent No's. 5,951,698 and 5,889,943

The Getting Started Guide for Trend Micro™ ScanMail™ for Lotus™ Notes is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about using specific features within the software are available in the ScanMail online help file, in the readme.txt, and from SolutionBank, Trend Micro's Web-based knowledgebase of technical product information.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at **docs@trendmicro.com**. Your feedback is always welcome.

To comment upon this documentation, go to the following Web site:
http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Chapter 6: Performing Manual and Scheduled Database Scans

Chapter 7: Using eManager

Chapter 1

About ScanMail™ for Lotus Notes

ScanMail for Lotus Notes works in real time to prevent viruses and malicious code from entering your Lotus Notes network via mail, replication, or infected documents. In addition, ScanMail's companion product, eManager, blocks spam mail and provides messages filtering based on content, size, domain, status, or whatever search criteria you specify.

ScanMail is also fully compatible with Control Manager, Trend Micro's centralized management console that lets you aggregate disparate antivirus protection into a cohesive solution. If you are adding ScanMail to an existing Control Manager network, see Appendix 1 for more information.

Documentation set

This Getting Started Guide acquaints you with the main features of ScanMail, guides you through the installation planning and steps, and then walks you through the basics of configuring both ScanMail and eManager to function according your needs.

Although this Getting Started Guide document discusses ScanMail in a Windows environment, the main ScanMail features and tasks are common to all platforms and so this guide serves to explain them all. *For platform-specific issues and/or installation instructions, see the readme.txt accompanying the software*.

Other documents in the set include: :

- **Readme.txt**—contains platform specific installation instructions, version enhancements, basic installation information, known issues, release history
- **on-line help**—contains usage advice, feature- and field-specific product information, and how to's
- **Knowledge Base**—a searchable database of known product issues, including specific problem-solving and troubleshooting topics; accessible at

  `http://solutionbank.trendmicro.com`

- **Electronic (.pdf) version**—of the printed manuals are available at
  `http://www.trendmicro.com/download/documentation/`

Supported platforms

ScanMail supports the Windows and Unix platforms listed below. For a detailed list of hardware and OS requirements, check the ScanMail on-line help database or see the readme.txt file. Currently, eManager is only supported on the Windows platform.

- Windows 2000 and Windows NT
- Linux (Red Hat 6.2 and SuSE 6.4 - Kernel ver. 2.4 and later)
- Sun Solaris
- IBM AIX
- IBM S/390
- IBM AS/400

Step-by-step instructions for installing ScanMail on each of the UNIX platforms above can be found in the readme.txt file.

Viruses in a Notes environment

ScanMail for Lotus Notes stops the spread and acquisition of computer viruses—both known and unknown—in the Lotus Notes client-server environment.

ScanMail provides constant detection and protection of the three points of entry where the Notes client environment is most vulnerable:

- **Email transmissions —** ScanMail performs real-time scanning on all inbound and outbound email messages and their attachments to stop viruses from entering

your system, or infecting someone else's (for example, a customer). The real-time Mail Scan task is called `tmmscan`.

- **Client database accesses —** ScanMail monitors database files that are modified in real time to prevent viruses from being archived among your stored database documents.
- **Replications** — ScanMail checks all files modified through the Notes database replicator in real time to keep viruses from being replicated from other Notes servers. The Real-time Database Scan task is called `repscan`.

In addition, ScanMail helps end the cycle of recurring infections with manual or scheduled sweeps of the entire database and mail message attachments.

About Scan tasks

Trend Micro Inc. is dedicated to providing integrated virus protection solutions that cover all the places where viruses may be hiding. The Notes environment is particularly complex due to its many features and capabilities. The same functions that allow users to easily exchange email, documents, and entire databases with other local or remote users also allow virus proliferation.

ScanMail includes two real-time scan tasks that load whenever the Lotus Domino Server is started: `pscan`, which checks read/write activities to the database and replications, and `tmmscan`, which checks all inbound and outbound email attachments *before* they are distributed to individual mailboxes, eliminating repetitive scanning of messages.

The task `dbscan` is available for Manual Scan and Scheduled scans.

ScanMail provides central configuration with remote management from any Notes workstation. Trend Micro's "CascadeUpdate" Technology automatically downloads new pattern files to the lead server and distributes them to all other servers using the Notes replication process. Each server automatically adopts new virus pattern files without the need for server reboot.

About viruses

Simply put, a computer virus is a program that replicates. To do so, the virus will need to attach itself to other program files (for example, .exe, .com, .dll) and execute whenever the host program executes.

Beyond simple replication, a virus always seeks to fulfill another purpose: to cause damage. Called the damage routine, or payload, the destructive portion of a virus can range from overwriting the partition table on the main system disk to scrambling the numbers in your corporate spreadsheets to just taunting you with sounds, pictures, or effects.

Related to viruses, are worms, Trojan horse programs, script bombs, and a host of other malicious programs designed to destroy data, crash the mail server, or otherwise interfere with the business of innocent companies and users.

It’s worth bearing in mind, however, that even without a "damage routine," left unabated, viruses and the other malicious programs will continue to propagate—consuming system memory, disk space, slowing network traffic and generally degrading performance. Often buggy, virus code can also be the source of mysterious system problems that take weeks to understand. Whether it was written to be harmful or not, a virus on your system can lead to instability and must not be allowed to remain.

Some viruses, in conjunction with "logic bombs," do not make their presence known for months. Instead of causing damage right away, these viruses do nothing but replicate—until the preordained trigger day or event when they unleash their damage routines across the network.

It is for this reason, that, immediately after installing ScanMail and updating the virus pattern file, you should run a complete scan of all your Notes databases—you need to be sure there are no viruses buried somewhere deep within your data.

About the virus pattern file

As new viruses are written, released to the public and discovered, Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file. Because new and virulent viruses are discovered every day, Trend Micro frequently makes available new versions of the virus pattern file, sometimes as often as daily, depending on the need and threat-risk.

ScanMail for Lotus Notes draws upon this database of virus "signatures", commonly called the virus pattern file, to detect viruses in email traffic, database replications, and database documents.

You can configure automatic updates of the pattern file to stay protected against the latest viruses. The updates can take place directly from the Internet, or by replication from a central server that holds the most current pattern files.

If a particularly damaging virus is discovered “in the wild,” or actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available (usually within a few hours).

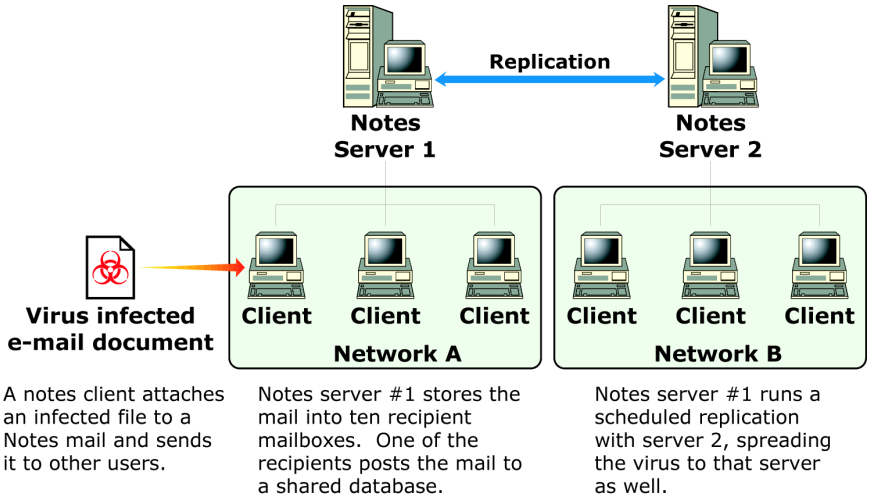


FIGURE 1-1. Risk: one virus-infected file can rapidly spread throughout an entire Notes network via daily Notes functions.

About the Scan Engine

At the heart of all Trend Micro products lays a proprietary scan engine, capable of quickly detecting all viruses known to be “in the wild”, or actively circulating. In addition, the engine detects Distributed Denial of Service (DDoS) attacks, and mass mailing worms/viruses such as Nimda, CodeRed, ILOVEYOU, and KLEZ.E.

Data is checked for viruses using Trend Micro’s 32-bit, multi-threaded scan engine and a process called pattern matching. In addition, whereas most antivirus companies

are limited to only one or two types of heuristic scanning, the Trend Micro scan engine employs multiple sophisticated algorithms to allow the quick identification of previously unknown Macro, Script, Boot, DOS, and polymorphic viruses.

The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help manage bandwidth).

Management features

ScanMail for Lotus Notes can be configured from the Notes client or through a Web browser. The Notes client provides the most convenient, easy-to-use interface to configure ScanMail because it provides the local access rights needed for some of the advanced options.

Notes script scanning

New types of malicious scripts are emerging that can be just as destructive as viruses. LotusScript provides a scripting language for the Notes environment. It is an event-driven, embedded scripting language with object-oriented extensions. Event-driven programming allows the automation of tasks such as opening databases, documents, and views; clicking buttons, prompting for user input, checking data entry errors, or preventing certain actions. LotusScript is a powerful tool that allows much customization of Notes tasks and is a real time-saver.

ScanMail employs script scanning to eliminate malicious code at the source before any damage can be done. ScanMail provides protection against destructive, powerful Notes scripts and macros contained in hotspots, otherwise known as "script bombs". User-definable destructive commands are blocked from execution, including functions, commands, script strings, and URLs.

Rich Text and Stored Form hotspot scanning

Notes hotspots allow the communication of additional information in a Notes document. Hotspots can display popup text, switch to a link, or perform a Notes action. Hotspots can provide much useful information and simplify Notes routines. Notes provides five types of hotspots: Link Hotspots, Text Popups, Formula Popups, Buttons, Action Hotspots.

However, hotspots can also be used for destructive purposes. ScanMail for Lotus Notes protects the Notes environment against the execution of malicious hotspots.

ScanMail for Lotus Notes provides the option to protect the two main categories of hotspots (either of which can contain the five main types listed above):

- Rich-text Hotspots
- Stored Form Hotspots

Rich-text hotspots are created as part of the original data saved in a document. Notes also provides the ability to store the original data entry forms with each document. These forms are called Stored Forms. ScanMail also protects against malicious hotspots stored in the body of Stored Forms, which is in rich-text format.

Advanced database scanning features

ScanMail for Lotus Notes supports multithreading using Trend Micro's proprietary scan engine. ScanMail scans UUencode, BINHEX, and MIME encoded attachments and a wide variety of compression types.

Enhanced scanning options

ScanMail for Lotus Notes provides the following enhance options:

- Performs virus scanning in memory, significantly increasing the scanning speed (must be enabled)
- Trusted Server Scanning for multiserver email and documents — mail or documents that have already been scanned on trusted servers will not be rescanned
- Separate treatment options are available for viruses versus script bombs found
- Separate temporary directories for Mail Scan, Manual Scan, Scheduled Scan, and Real-time Database Scan can be configured
- Strips macros from Office documents to prevent malicious macros from running
- Scans Microsoft Office objects that have been embedded in documents, for example, OLE objects. Removes objects containing malicious code
- Ability to exclude specified directories during Manual and Scheduled scans

Incremental scanning

Setting the Incremental scanning option during Manual and Scheduled database scans saves considerable server time and resources. Incremental scanning allows selective scanning of new and newly modified documents. Scanning will be performed only on files that have not been previously scanned or that have been altered since the last scan.

Database scan execution order

ScanMail for Lotus Notes now offers many database scanning features in addition to virus scanning. The scan order is as follows:

1. **Incremental Scanning** (Manual and Scheduled Scan) — if documents have previously been scanned, they are not rescanned.
2. **Scanning Embedded Objects** — scan Microsoft Office objects that have been embedded in mail messages for malicious code.
3. **Stripping macros from Office documents** — strips potentially destructive macros from Microsoft Office documents.
4. **Virus Scanning** — attached files containing viruses are cleaned, passed, quarantined, or deleted as specified. A notification message can be sent to the Administrator or other specified users.
5. **Script Scanning** — Notes hotspots in stored forms and rich text fields are scanned for malicious script commands and URLs. If destructive code is found, the hotspot can be cleaned, passed, or deleted. The hotspot can also be replaced with a customizable message and a notification message can be sent to the administrator(s).

Advanced email advanced scanning features

ScanMail for Lotus Notes offers the capability to perform advanced email scanning, including reducing total scanning by not rescanning documents already scanned by trusted servers. Included also is the ability to block specified file extension names and/or file extension types from delivery within your Notes environment.

Trusted server scanning

Setting the Trusted Server Scanning option for real-time email scanning saves server time and resources by allowing the configuration of trusted servers. Documents scanned on trusted servers need not be scanned again.

"Red Alert" attachment blocking

ScanMail for Lotus Notes includes the ability to block certain attachments from being delivered. This feature can be used in "Red Alert" virus outbreak situations, or simply used to enforce existing company policy on file types that can be sent.

The types of files blocked are user-definable and can be documents, executables, drivers, script files, or any other file name and/or file extension type. In addition, you can configure a recipient exclusion list so that certain users, such as the IT department, will receive all attachments.

Block action

The Mail Scan Block action prevents messages containing infected files from being delivered. The entire email message is blocked from delivery, including the text, header, and all attachments.

This action is more complete than the Delete action, which deletes infected attachments only. The original message text of the email and any uninfected files are still delivered to the intended recipient.

Email Filter rules

The Email Filter works to check email messages for domain restrictions. With the use of Filter Rules, email messages sent to and from specified domains can be blocked in general, blocked based on mail size, delayed in certain business or non-business hours, or set to low priority. In addition, you can enable Subject line blocking if you would like to block email from delivery based on text in the subject line.

Multiple rules can be set with individual notification messages. In addition, you can configure a sender exception list so that critical staff members can be excluded from mail blocking.

The ScanMail Time Database, `smtime.nsf`, is used for the Email Filter Rule option to send attachments at a specified time. This option enables bandwidth

management, for example, postponing delivery of large attachments until after normal working hours.

Regular and rich text notification

In all configurations, you can use ScanMail's default message or compose one of your own. You can choose to send regular text ScanMail notification messages or use the new rich text format. Rich text format is used to customize the background, graphics, and text style of notifications.

Separate internal and external notifications can be configured in the warning message sent to the sender and recipient(s) when you use regular text notification.

Email scan execution order

ScanMail for Lotus Notes now offers many email scanning features in addition to virus scanning. The scan order is as follows:

1. **Email Filter Rules** — if email matches a filter rule, the specified action is triggered (block always, block if a specified size, set to low priority, etc.).
2. **Trusted Server Scanning** — if mail has previously been scanned on specified servers, it is not rescanned.
3. **Attachment Blocking** — mail attachments are compared with the extension block list; matching files are blocked and not scanned.
4. **Scanning Embedded Objects** — scan Microsoft Office objects that have been embedded in mail messages for malicious code.
5. **Stripping macros from Office documents** — strips potentially destructive macros from Microsoft Office documents.
6. **Virus Scanning** — attachments are scanned for viruses and the action specified is taken.
    - Viruses detected — mail attachments containing viruses are cleaned, passed, quarantined, or deleted. Alternatively, the entire message can be blocked from delivery. Notifications can be sent to the Administrator, sender, or recipients
    - No viruses detected — mail that does not contain viruses can have a "Safe Stamp" inserted in the Subject line to indicate that it was scanned

- Encrypted mail — a message with attachments that can't be scanned due to encryption can have an Encryption Stamp inserted in the Subject line to indicate that they were not scanned
- Office macro strip notification — if stripping Office macros is enabled, messages that have had macros stripped can have a notification stamp
- Disclaimer — if a Disclaimer Stamp is configured, it will be inserted in all mail that has been scanned for viruses

7. **Script Scanning** — Notes hotspots in stored forms and rich text fields are scanned for malicious script commands and URLs. If destructive code is found, the hotspots can be cleaned, passed, or deleted. The hotspot can also be replaced with a customizable message and a notification message can be sent to the administrator(s), sender, and/or recipient(s).

Stopping email delivery when ScanMail is not running

You can configure whether or not to have Notes continue mail delivery if the ScanMail tasks are stopped. By default, when ScanMail is not running, mail will continue to be delivered by the Notes server. The variable SMStopMail in the `notes.ini` file is used to configure whether to continue mail delivery when ScanMail is stopped.

Virus and quarantine logs

Individual virus log records contain a unique ID number for the document. They contain information on the server and database the document was found on, the attachment name and action on viruses found (or files blocked, or script bombs found).

ScanMail includes a variable called SMOutputLevel in the `notes.ini` file that you can set for different logging levels. This variable controls the recording of virus information messages in the Notes system log and includes ScanMail task activity such as the databases scanned.

Quarantine database

ScanMail for Lotus Notes features a database for storing quarantined documents to prevent users from accidentally these files. The quarantine database contains live viruses, so it is a good idea to delete the quarantine records periodically.

Virus statistics

ScanMail for Lotus Notes provides several lists of viruses most frequently detected on your network, the Virus Statistics table which is familiar from earlier versions of ScanMail, and the database history.

- **Virus Charting**—list of top 10 viruses detected
- **Database Charting**—list of top 10 databases infected
- **User Charting**—list of top 10 users sending the most viruses
- **Virus Log Statistics**—information on script bombs detected and files blocked in addition to disposition of viruses detected
- **Database History**—information about the scanning history and number of documents scanned

Chapter 2

Installing and Accessing ScanMail

For uniform antivirus protection, install one copy of ScanMail on each Notes Domino server in your Notes network. After installing, be sure to update the virus pattern file so your protection is as current as possible and then follow the recommended database setup procedures described in chapter 3.

This chapter provides installation planning, step-by-step installation instructions for the Windows platform, and explains how to access the ScanMail consile locally, via Notes client, and remotely, via Web browser.

Step by step installation instructions for the Unix platforms can be found in the `readme.txt` file that ships with the product or on the Web:

- Sun Solaris
- Linux
- IBM AIX
- IBM OS/390
- IBM AS/400

Download the platform specific readme.txt, or more complete Getting Started Guide from:

`http://www.trendmicro.com/download/product.asp?productid=10`

System requirements

Always check the readme.txt to confirm version-specific requirements and for any last-minute news and product information. ScanMail supports the following platforms, detailed below:

- Windows, Linux, Linux zSeries, Solaris, AIX, AS-400, OS-390
- Lotus(TM) Domino(TM) R 5.x and above, Domino 6 and above

Note: The agent for Trend Micro's centralized management console, Control Manager, may have system requirements that differ from the above. Before installing the agent, check its system requirements in the age-specific readme file.

Windows

ScanMail and eManager have the following system requirements.

- Microsoft Windows 2000 server, or Microsoft Windows NT 4.0 w/ SP3 or later
- Server with a Pentium processor
  - 64MB RAM (256MB recommended)
  - 20MB available disk space for program files
  - 100MB disk space for swap files (500MB recommended)
- Internet access (for pattern downloads) on at least ScanMail server

Linux

The following Linux platforms are supported:

- RedHat 6.2 (Kernel version 2.4 or later recommended)
- SuSE 6.4 (Kernel Version 2.4 or later recommended)
- Linux for IBM zSeries 8 + Service Pack 2

- Internet access (for pattern downloads) on at least ScanMail server

Solaris and AIX

In addition to the hardware specified above,

- Solaris 2.5.1 or later (or)
- AIX 4.1.5 or later
- Internet access (for pattern downloads) on at least ScanMail server

AS-400

In addition to the hardware specified above,

- AS/400 Version 4, Release 5 or later
- 128MB RAM
- 350MB disk space available for program files;
- 100MB disk space available for swap files
- Internet access (for virus pattern file, scan engine and spam rule downloads)

0S-390

In addition to the hardware specified above,

- OS/390 2.10 or above
  128MB RAM
- 64 MB disk space available for program files;
- 100 MB disk space available for swap files
- Internet access (for virus pattern file, scan engine and spam-file downloads)

Using ScanMail for Lotus Notes with Trend Virus Control System and/or Control Manager

You can install the Control Manager 2.5 agent for ScanMail on a Windows server. It does not need to be running Lotus Domino, or the Notes client.

- Intel™ Pentium™ 300MHz processor (or higher recommended)
- 128MB RAM minimum (256MB or more recommended)
- 50MB free disk space for the program files
- Control Manager 2.5 Server

Note: Uninstall Trend Virus Control System if you plan to install the Control Manager 2.5 agent on a domino server

---

It is recommended that the Server.id of the Domino Server have no password if you are installing a Control Manager agent.

Installing ScanMail™ for Lotus Notes

Installing ScanMail for Lotus Notes is quick and easy. There are really only a few things to keep in mind:

- ScanMail must be installed to the Notes data directory, *not* to its own directory. The installation program seeks out the program directory.
- Before installing, stop the Notes server and close the Notes client if it is open.
- If you are upgrading to ScanMail version 2.6 from ScanMail version 2.5x, there is no need to uninstall the existing copy—just run the Setup.exe program and you will be upgraded automatically

---

Note: If you are running a version of ScanMail prior to 2.5x, uninstall it before installing version 2.6.

To install ScanMail on a Windows 2000 server:

1. If you have the Trend Micro Enterprise Protection CD,

a. Insert Disk 1 in the CD drive of the Notes server where you will install ScanMail and, when prompted, select the language you want to use. (If the CD does not automatically open, double-click the file ***go.exe*** in the root directory of the CD drive).

b. Next, click **Choose Software** in the Welcome screen that appears, and then choose **ScanMail for Lotus Notes** from the list of product families and **ScanMail for Lotus Notes (Windows)** from the list of platforms.

c. Click the **Install** button to begin installing ScanMail, or **Documentation** to view the readme.txt.

- If you are downloading from the Web:

  a. Download or copy the ScanMail binary archive to a temporary directory on the Notes server where you want ScanMail to run, and then extract the files.

  b. Double-click the file **setup.exe** to begin installing (or **readme.txt** for program information).

2. In the **Welcome** window appears, click **Next**.to continue, and then **Yes** to accept the Trend Micro License Agreement.

3. Follow the on-screen prompts to identify the location of your **`notes.ini`** file (typically in `\lotus\domino`), and identify where the ScanMail program files and databases should be installed (typically in `\lotus\domino\data`).

4. After specifying where to copy the ScanMail files, enter your name and company. Click **Next**, and enter a product serial number.

Note: Serial numbers for both ScanMail and the optional plug-in eManager can be found on the outside front cover of the Getting Started Guide or obtained from *sales@trendmicro.com*. If no serial number is entered, a 30-day trial version of the product(s) is installed.

---

5. After copying all the program files, Setup will sign the ScanMail databases just installed using the Notes **server.id**—Click **No**, unless you specifically want to use a different ID. *If you choose to sign the databases using another ID, be sure it is administrator-level*.
6. Next, choose the temporary directories you want ScanMail to use when scanning, or just click **Next** to accept the defaults:

```
lotus\domino\data\smln\SMTemp\MailTemp—Mail Scanning
lotus\domino\data\smln\SMTemp\DbTemp—Manual Scanning
lotus\domino\data\smln\SMTemp\PTemp—Scheduled Scanning
lotus\domino\data\smln\SMTemp\RepTemp—Real-time Scanning
```

> **Note:** If you are running ServerProtect or some other antivirus product on the Domino server where you will install ScanMail, be sure to exclude from scanning ScanMail's temp directories. Otherwise, a scanning conflict can occur.

7. Setup takes a few minutes to sign the ScanMail databases just installed. Once they have all been signed, click **Finish** to complete the installation and view the `Readme` file.
8. Restart the Notes Domino server to start the ScanMail tasks and begin scanning.

See also: *Upgrading from the Trial Version*, *Installing on a Partitioned Server*, and *Installing a Control Manager Agent for ScanMail*.

Upgrading from the trial version

The 30-day free trial version of ScanMail is fully functional. After 30 days, however, the scanning services will continue to load but are disabled. In this case, you should either remove ScanMail or obtain a license. Obtain a serial number by purchasing the upgrade, or visit the Trend Micro Web site for purchasing information at:

```
http://www.trendmicro.com/buy/us/enterprise.asp
```

Installing ScanMail to a partitioned server

When installing multiple instances of ScanMail onto a Domino partitioned server, all ScanMail executable files are installed to the same Notes directory—all instances of ScanMail installed on a the same machine will use the same executable files.

Not so for the ScanMail database files, however. For the data files, each partition of ScanMail maintains its own database files and temporary directories, the location of which are defined in each partitions's respective n`otes.ini` file.

Install ScanMail on a Domino partitioned server as you would any "normal" installation, but with these differences:

- If you will be installing an agent for Trend Micro Control Manager, stop the Domino server, install ScanMail on all the partitions, restart the Domino server, and then install an agent on each partition with ScanMail.
- Specify a unique name for the data directory and temporary directories. For example:

```
\Lotus\Domino\Data1\smln\SMTemp\MailTemp–Mail Scanner
\Lotus\Domino\Data1\smln\SMTemp\RepTemp–Real-time Scanner
\Lotus\Domino\Data1\smln\SMTemp\DbTemp–Manual Scanner
\Lotus\Domino\Data1\smln\SMTemp\PTemp–Scheduled Scanner
```

- Repeat the installation for each partitioned server that you have installed. For example, locate the "notes.ini" for the second partitioned server.
- When prompted, choose "Overwrite" to install to additional partitioned servers and specify a unique name for the data and temp directories for each.:

```
\Lotus\Domino\Data2\smln\SMTemp\MailTemp–Mail Scanner
\Lotus\Domino\Data2\smln\SMTemp\RepTemp–Real-time Scanner
\Lotus\Domino\Data2\smln\SMTemp\DbTemp–Manual Scanner
\Lotus\Domino\Data2\smln\SMTemp\PTemp–Scheduled Scanner
```

Note: If you are running ServerProtect or some other antivirus product on the Domino server where you will install ScanMail, be sure to exclude from scanning ScanMail's temp directories on each partition. Otherwise, a scanning conflict can occur.

Opening the ScanMail console

You can administer ScanMail locally, from a Notes client, remotely, via Microsoft Internet Explorer browser, and in conjunction with other Trend Micro antivirus products via the Trend Micro Control Manager.

Using a Notes client

To open the ScanMail console from a Notes client on the ScanMail server:

- Right-click the Notes Workspace, choose **Open Database** in the pop-up menu that appears, and use the **Browse** button to locate the file:

  `\Lotus\Domino\Data\smconf.nsf`

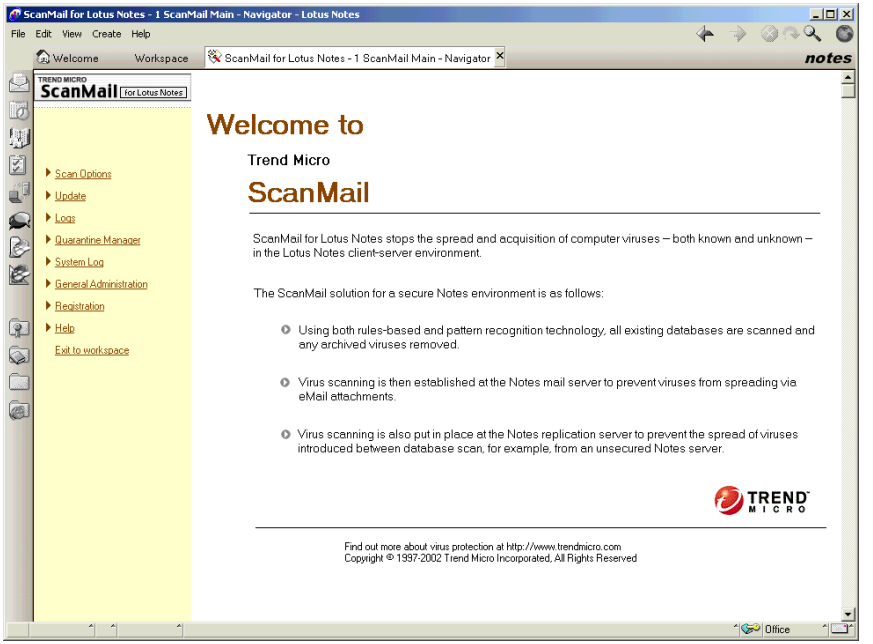


FIGURE 2-1. The ScanMail Welcome screen, as seen from a Notes client.

Double-click the ScanMail icon in the Workspace to open the console, and the Welcome screen appears with the main menu in the left navigator pane. From each menu page, return to the main page by clicking the **Cancel** button in the Action bar at the top of the screen, or by pressing the **Esc** key.

Using a web browser

To open the ScanMail console with a Web browser:

1. In the **Address** bar, specify the URL address below:

   `http://<computer>/smconf.nsf`

   where **`<computer>`** is the name or IP address of the server. Press **Enter**. If you have changed the port number, you should enter it as well. For example, if you have changed the port to 8080, you would enter:

   `http://123.123.123.12:8080/smconf.nsf`

2. If prompted for a **User Name** and **Password**, enter a Person and Internet password as specified under **People** in the Notes Name & Address book.

3. The ScanMail for Lotus Notes main menu appears. Make your selections from the left navigator pane.

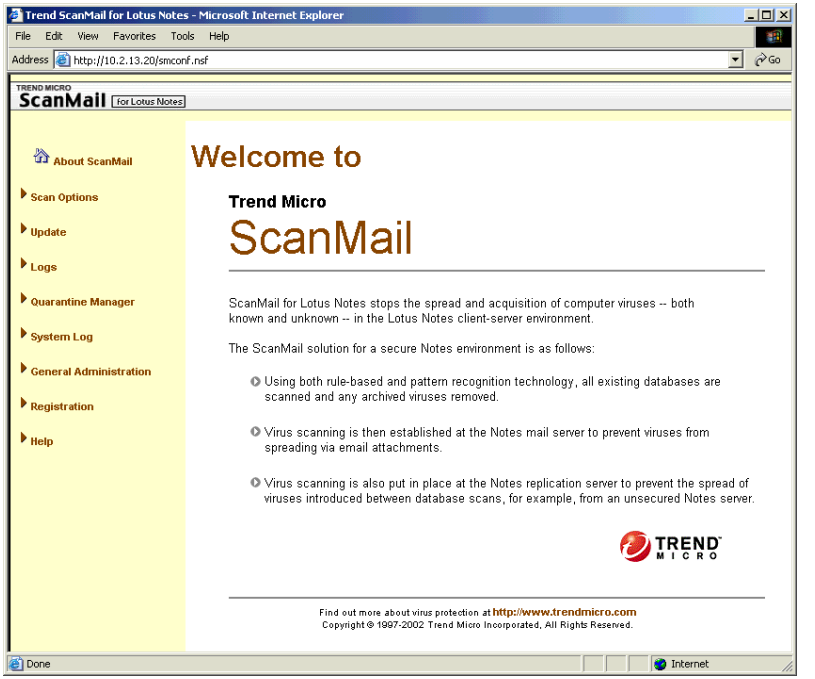


FIGURE 2-2. The ScanMail Welcome screen, as seen from a Notes client.

Using a Control Manager agent

See Chapter 10 of this document for information about Trend Micro Control Manager, agent installation instructions, and how to access ScanMail via the Control Manager console.

About Control Manager

Trend Micro Control Manger is a Web-based management tool that allows administrators to configure, monitor and maintain most antivirus software installed on the network from a single console—regardless of location or platform.

TMCM can be individually purchased. Information on using ScanMail in a Control Manager network can be found on ScanMail's on-line help and in Chapter 10: *Control Manager.*

Removing ScanMail for Lotus Notes

Before removing ScanMail,

- Make sure that the Notes server and client are not running
- If you installed the Trend VCS agent for Lotus Notes, you should uninstall that first before removing ScanMail. See the online Help database for further information.

To uninstall, click the **Start** button and choose **Programs | Trend ScanMail for Notes | Uninstall Trend ScanMail for Lotus Notes 2.5**. ScanMail's uninstall program will remove shared and standard program files, as well as program folders, items, directories, and entries made to the registry.

If the ScanMail Icons on the Workspace still appear after uninstallation, right-click on each and choose **Remove From Workspace** from the menu that appears. In addition, you can remove the ScanMail entries in the `notes.ini` file manually.

Note: Changes to the ScanMail `notes.ini` variables will not be automatically removed by uninstallation.

Chapter 3

Using, Updating and Optimizing ScanMail for Lotus Notes

Once ScanMail is installed, make sure you do the following:

- Add the ScanMail program icons to your Workspace and restrict access to the ScanMail databases
- Configure ScanMail to recognize a proxy server (if any) on the network
- Update the virus pattern file and scan engine
- Register your copy of ScanMail with Trend Micro
- Optimize performance by enabling memory-based scanning and establishing multiple scan threads

---

Note: After installing ScanMail and restarting the Notes server, ScanMail automatically loads its scan tasks and begins real-time scanning of Notes mail traffic and database activity.

This chapter provides information on using, updating and optimizing ScanMail -- all tasks you should undertake before scanning all of your Notes databases. Subsequent chapters provide information on how to configure mail and database scans, run a complete scan, and see ScanMail work by using a special test "virus".

Configuration examples given in this manual are from the Notes client—certain ScanMail configuration changes can only be performed from the Notes client.

Adding the ScanMail Icons to the Workspace

After installing ScanMail, you can access program links to the readme.txt and ScanMail uninstall utility in the Windows **Programs** menu (under Trend Micro ScanMail for Lotus Notes). Adding the ScanMail program Icons to the Notes Workspace must be done manually.

To add the ScanMail icons to a Workspace:

1. Make active the Workspace that you want ScanMail to be accessible from. Right-click and select **Open Database...** in the popup menu that appears.
2. Click **Browse** and locate the `/Lotus/Domino/Data/` directory, where you can **Select** the following databases to be opened

   smconf.nsf— main configuration database
   smquar.nsf— Quarantine Logs database
   smhelp.nsf— Help database
   smency.nsf— Pattern database

   smftypes—database listing recognized file types (does not need to be added to the Workspace).
3. After adding the icons to the Workspace, double-click **ScanMail for Lotus Notes** to open the console.

Restricting access to the ScanMail databases

We recommend that you restrict access to the ScanMail databases so that the casual user of the Notes network is not able to change your ScanMail configurations or delete log files. You can restrict access using Notes' native access control.

To restrict access to the ScanMail databases:

1. Right-click on each **ScanMail** icon and in the pop-up menu that appears, click **Database > Access Control...**.

2. Locate **-Default-** at the top of the list and select it if it is not already highlighted. Find **User type** and **Access** in the upper right corner.

   - For User type, select **Unspecified**.
   - For Access, select **No Access**.

3. As Notes Administrator, you need full rights to administer the ScanMail database.
   a. Your name should appear in the same list as **-Default-** was found. If it does not, click the **Add** button, and then the "look up" silhouette on the right.
   b. Choose your name from the list that appears in the **Names** window and click **Add**. Click **OK** when your name appears in the **Added** pane on the right side of the **Names** window.
   c. In the **Access Control List** window, highlight your name and click the drop-down arrow for **User type**, select **Person**. Do the same for **Access**, but give yourself **Manager** access.
4. The Notes server also needs full rights to access the ScanMail database.
   a. Click the **Add** button, and then the "look up" silhouette on the right.
   b. Choose the server name from the list that appears in the Names window and click **Add**. Click **OK.**
   c. In the Access Control List window, select the server, click the drop-down arrow for **User type**, and select **Server**. Do the same for **Access**, but give the server **Manager** access.
5. Check the access status of any other people who appear on the list. We recommend that you give no higher than **Reader** access to most users unless they share Notes administrative duties. Click **OK** to save the configuration changes.

Configuring ScanMail to work with a proxy server

If there is a proxy server on the network between ScanMail and the Internet, you will need to identify the location and provide valid log in credentials before performing any virus pattern, scan engine, or spam database updates.

Likewise, you will need to identify the proxy location before registering ScanMail.

To set ScanMail to work with a proxy server:

1. Click **Update | Update Setting** and then go to the **Proxy Server Settings** portion of the page that appears.
2. Select the type of proxy server on your network, HTTP or SOCKS, and then provide the proxy's IP address and port number. Also provide any login credentials that may be required to access the machine.

   Missing or incorrect proxy server settings can cause one or more of the following error messages to appear:

   - Error: Unable to resolve server IP -- DNS error or server not found
   - Error: HttpConnection: Unable to create socket connection
   - Error: TmDownloader: Unable to open resource
   - Error: TmDownloader was unable to download file http://smln-t.activeupdate.trendmicro.com/activeupdate/server.ini to [path]
   - Unable to open resource
   - Generic network error

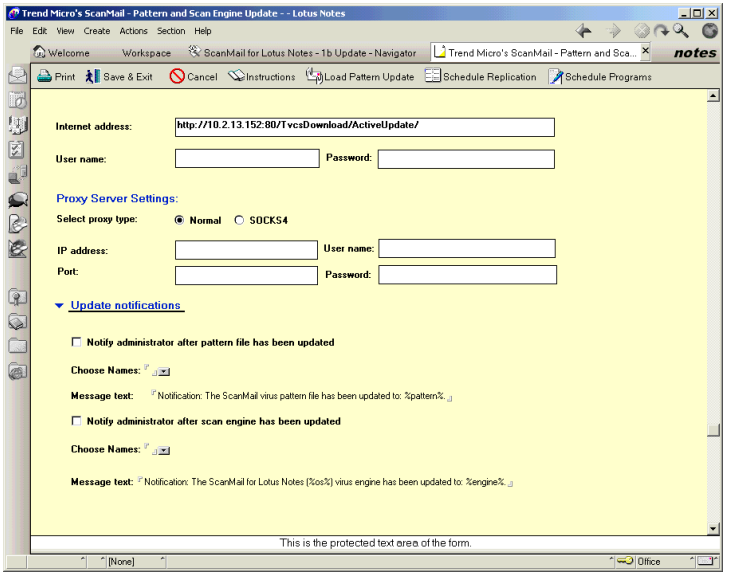


Figure 3-1. To verify that the proxy server settings you entered are correct, you can use a "ping" command from a DOS prompt using the IP address and port number.

Registering ScanMail

You must register ScanMail to obtain virus pattern file and other updates.

To register ScanMail:

1. After identifying your proxy server (if any), click Registration in the main ScanMail menu.

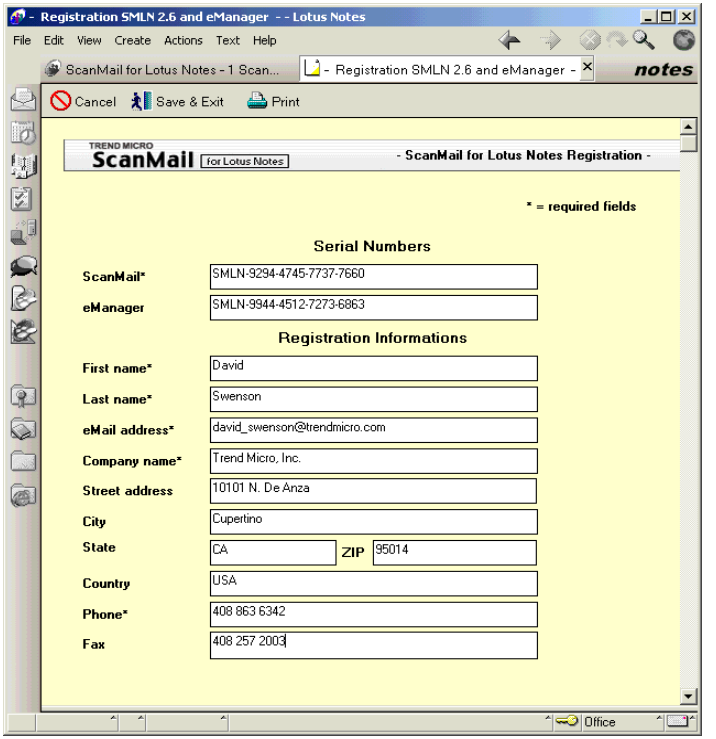


FIGURE 3-2. It is important to register your copy of ScanMail.

2. Enter your product serial number for both ScanMail, and eManager (optional, but required for spam and content filtering).

Note: Serial numbers can be found on the registration card inside the ScanMail box, on the cover of the Getting Started Guide, or obtained by contacting sales@trendmicro.com.

3. Fill out the remaining contact information, and click **Save & Exit** to return to the previous screen.

Viewing current versions

It is important to keep the ScanMail virus pattern file, scan engine, and if eManager is installed, spam database up to date.

To check which version of the ScanMail program, scan engine, and virus pattern file you are using:

1. From the main ScanMail menu, click **General Administration** > **Program Status.** A list of ScanMail servers appears, and for each the version of program files, scan engine, and virus pattern file is displayed.

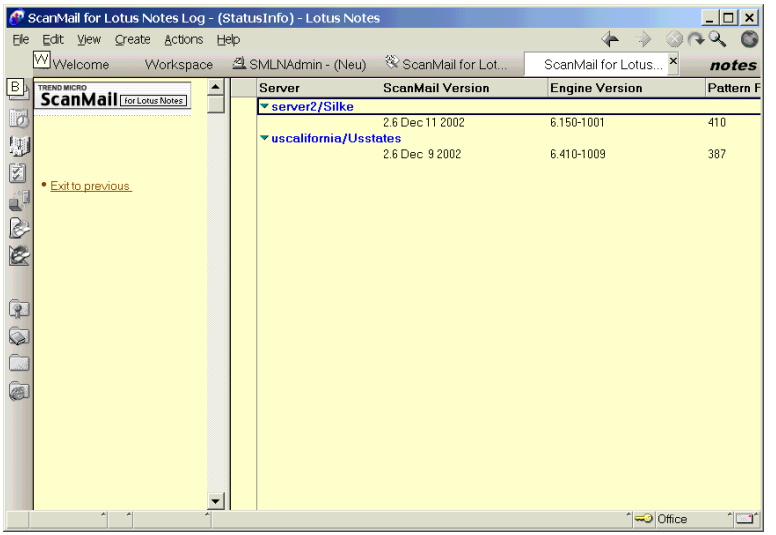


FIGURE 3-3. A summary of current versions is available by clicking General Administration > Program Status in the main ScanMail menu.

2. Double-click an entry in the list to open the Program Status window, and expose the following details:
   - ScanMail version
   - ScanMail build number
   - Scan engine version
   - Spam filter version
   - Current virus pattern version
   - Virus pattern version in Pattern database
   - Mail scan status
   - eManager status
   - Real-time scan status

Checking the anti-spam database version

eManager users can also check the version of the anti-spam database they are using. Anti-spam updates may be made available as often as once a day.

To check the version of the anti-spam database you are using:

- From the main ScanMail menu, click **Update > Pattern Database > Spam Database > Current Spam Database**. The spam database version is displayed.

Note: **Virus pattern version in smency.nsf** lists the pattern file stored in the pattern file database. This pattern file is updated from the ScanMail interface through Internet or Replication. If you manually copied a pattern file into the Notes or Domino directory, it will not be displayed here.

About the virus pattern file

Thousands of new viruses are written and released each year, and you should not allow the pattern file to fall out-of-date. In fact, you should schedule virus pattern file updates no less than once a week; checking for updates daily is also recommended.

ScanMail for Lotus Notes draws upon an extensive database of virus "signatures", commonly called the virus pattern file. ScanMail uses this file to detect viruses in email traffic, database replications, and database documents. As new viruses are written, released onto the public, and discovered, Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file.

The virus pattern file is stored in the Pattern database, `smency.nsf`. You need to register ScanMail before you can update the virus pattern file, and updates are available free for a year to registered ScanMail customers.

Updating the virus pattern file

Although we recommend that you schedule automatic virus pattern updates, you can perform a "manual" update of the virus pattern file at any time—especially just after installing ScanMail.

To manually update the virus pattern file:

1. In the main ScanMail menu, click **Update > Update Setting**.
2. Next, under **Components**, deselect **Virus pattern** (and/or **Scan engine**).
3. Choose **ActiveUpdate server** for **Virus pattern files** (and/or **Scan engine**).

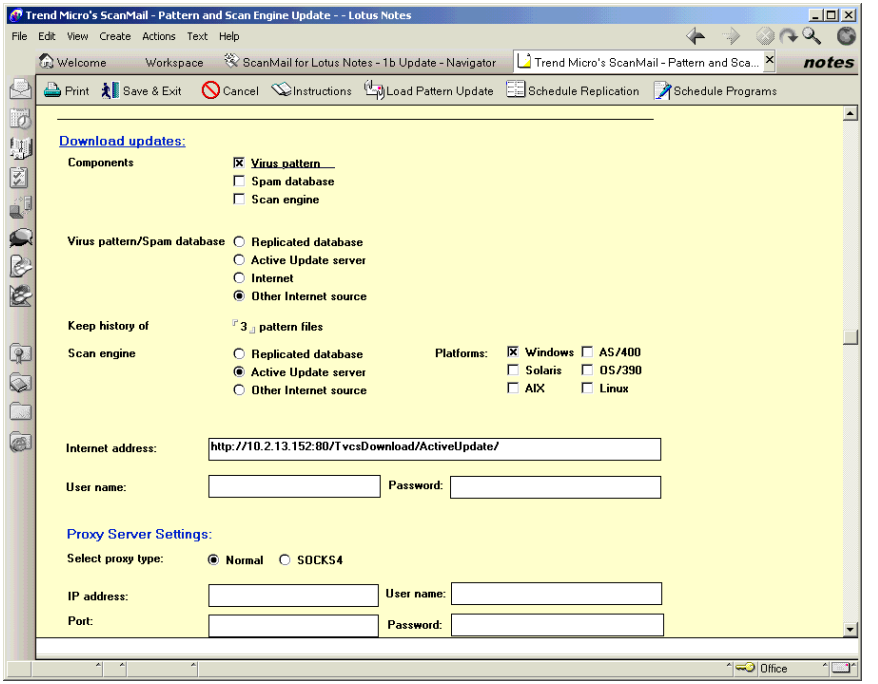


FIGURE 3-4. It is very important to keep your virus pattern file, scan engine, and spam database up to date.

4. In the **Internet Address** field, specify the URL for the ActiveUpdate sever. No **User name** or **Password** are required to access the ActiveUpdate server, so leave these fields blank.
5. If there is a proxy server on your network between the ScanMail server and the Internet, specify its IP address, port, and a user name & password for accessing it, and then configure your **Update notifications**.
6. Click **Load Pattern Update** on the action bar at the top of the screen and type
   `load pupdate`

in the server console command field that appears.

With **Live console** selected, or by viewing the Notes command window, you can monitor the progress of the update scripts.

The version number of the new virus pattern file is displayed, as is the number of the version you're replacing. When the download is finished, a confirmation message is displayed to verify that the procedure, which can take from a few seconds to a few minutes, was successfully completed.

Scheduling automatic virus pattern updates

Rather than download the entire virus pattern file each time, you can have ScanMail download only that part which is new since the last update. The feature is called ActiveUpdate, and it can save you as much as 95% of bandwidth typically consumed on these tasks.

In a multi-server environment, you can have every ScanMail server independently poll for virus pattern updates using ActiveUpdate, or you can designate a single ScanMail server to act as a central "clearing house" for downloading updates and then have your peripheral ScanMail servers pull in the update using replication.

Note: You must register ScanMail to perform virus pattern updates. A serial number is required to register and can be obtained by contacting **sales@trendmicro.com**

To enable ActiveUpdate:

1. From the main ScanMail menu, click **Update > Update Setting** in the ScanMail Configuration database.
2. Under **Download updates** > **Components** select or deselect **Virus pattern, Spam Database**, and/or **Scan engine** (depending on your needs).
3. Make sure that Active Update server is selected, and that you have filled out the proxy server settings if there is a proxy server on the network.
4. For Internet Address, accept the default:
   `http://smln-t.activeupdate.trendmicro.com/activeupdate`
5. Next, on the **Action** bar at the top of the page, click the **Schedule Programs** button and in the Address book that appears, click **Add Program** to open the Program window.

6. In the **Program name** text field, enter *pupdate*, and then click the **Schedule** tab to make it active and choose **Enabled**.
7. Choose a time and frequency for the update to occur, then **Close & Save** to close the Address book that was opened. Click **Close and Exit** again on the Pattern and Scan Engine Update page.

Note: Trend Micro frequently publishes Virus Pattern updates to stay current with newly discovered viruses. We recommend that you schedule *daily* virus pattern updates.

Using the EICAR test "virus" to see ScanMail work

After installing ScanMail you should test the setup to verify that it is working properly see how virus detection, notifications, etc. actually work.

The European Institute for Computer Antivirus Research, or EICAR has developed a test script that can be used to test your antivirus software. This script is an inert text file whose binary pattern is included in the virus pattern file from most antivirus vendors. *It is not a virus and does not contain any program code.*

WARNING! Never use real viruses to test your antivirus installation!

Disable any antivirus software running on your network or computer before attempting to download the EICAR test script or it will be detected as a virus and the download prevented!

Obtaining the Eicar test file

You can download the EICAR test script from the following URLs:

```
http://www.trendmicro.com/vinfo/testfiles/
http://www.eicar.org/anti_virus_test_file.htm
```

Alternatively, you can create your own Eicar test script by typing the following into a text file and then naming the file "eicar.com":

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H
*
```

Configuring ScanMail™ for optimal performance

Use memory-based scanning and/or multiple threads for faster scanning performance. Memory can be allocated to ScanMail for the following scan tasks:

- Replication Scanning
- eMail Scanning
- Scheduled Scans
- Manual Scans

Although there is no formula for determining the amount of memory to specify for memory-based scanning, a good rule of thumb is that the amount should be 1.5 to 2 times the size of the average large message passing through the mail server.

For companies who set a mail-size limit the choice is clear cut. If the average size of large messages is not known, you can either do some analysis to find out the size and frequency of large messages crossing the mail server, or "guesstimate" that allocating 5MB memory for mail scanning is sufficient to handle 97% of all mail processed, and that scanning the largest 3% of mail messages on the hard drive does impact performance.

Allocating the right amount of memory is especially important if you are running multiple instances of the mail scanning task, tmmscan. For example, if you decided to just give mail scanning 25% of the system's 256MB RAM, and if you decided to run 6 instances of tmmscan to keep up with traffic, not only would 99% of the allocated RAM never be used, but all tasks would default to the hard drive since the total exceeds available resources.

Notes:

- Memory is individually allocated, not aggregated or shared between tasks.
- Multiple instances of the same scan task each use their own block. To simultaneously process more than one message at a time, load multiple instances of tmmscan—each instance will occupy the amount of memory allocated.

Setting up memory-based scanning

Memory-based scanning is independently available for each of the four scan tasks, whenever the task is active. If you employ memory-based scanning for multiple scan tasks, make sure that the aggregate amount of memory dedicated to all tasks does not exceed system resources.

For example, 2MB for mail, 2MB for replications, 2MB for real-time, and 2MB for manual scans adds up to 8MB of memory. But only 4MB--that which is dedicated to real-time mail and database scan--is *always* reserved exclusively for ScanMail, whether or not the scanning for that task is actually occurring.

To configure memory-based scanning:

1. Open the **Scan Options** menu and choose the scan task you want to configure (Mail Scan, Replication Scan, Manual Scan, or Scheduled Scan).
2. Enter a whole number in the Scan Memory field.
3. Finally, click **Save & Exit** (or continue filling out the configuration form and then click Save & Exit).

Notes:

- To disable memory-based scanning, enter a zero in the scan memory field
- Multiple instances of the scan task will each have their own memory block

Creating multiple scan threads

You can create a multi-tasking scan environment by running more than one instance of `tmmscan` at the same time.

Running four instances of `tmmscan`, for example, can allow you to quadruple peak processing efficiency. Each instance of `tmmscan` loaded allocates the amount of memory specified in the **Mail Scan** configuration page.

Load additional tasks via command line, or by adding the command to the notes.ini file.

command line: `load tmmscan`

notes.ini: Open `notes.ini` using a text editor and modify the `ServerTasks=` line. For example:

ServerTasks=Router,Replica,Update,Amgr,Sched,AdminP,HTTP,POP3,**TmmScan, TmmScan,TmmScan,**RepScan

Scanning all databases

Notes databases can be scanned manually from the Notes/Domino server console or by using the ScanMail interface.

ScanMail's Manual scanning applies only to Notes databases. Although other types of files on the hard drive are not scanned, all file types contained within a Notes database can be checked for viruses, including OLE attachments.

Any Notes databases on a local or mounted hard drive, including network drives, can be included in a Database or Scheduled Scan.

- To scan databases from the Notes Command console, enter the following:

  ```
  load dbscan database.nsf
  ```

  where database.nsf represents the database you want to scan.

  ScanMail assumes as a default location the path specified under "Directory" in the notes.ini file on the Domino server.

- To scan multiple databases, delimit with spaces. For example:

  ```
  load dbscan database.nsf database2.nsf database3.nsf
  database4.nsf
  ```

Setting access rights to ScanMail (web browser)

To set up rights to access ScanMail from a Web browser:

- Enter your **HTTP proxy server settings**, if you use a proxy server to access the Internet.
- Set up **Rights to run unrestricted LotusScript/Java Agents**.
- Set up an **Internet password.**
- Load the **HTTP task** for Web access.

Each of these steps is described in detail in the following sections.

Setting up rights to run unrestricted LotusScript/Java agents

The user id that you are using must have rights to run unrestricted LotusScript/Java agents.

To set up rights to run unrestricted LotusScript/Java agents:

1. From the Notes Workspace, double-click the Address Book and then bring up the configuration document for the server where ScanMail is installed (via **Server | Servers**).

   Note: ScanMail requires that the Notes server be allowed to **Run unrestricted LotusScript/Java agents**. In addition, the users who access ScanMail through the Web should be listed here.

2. For Notes 4.x, locate and select **Agent Manager** to expose the Agent Restrictions options. For Domino 5.x, go to the **Security** tab, then scroll down to Agent Restrictions.
3. Double-click **Run unrestricted LotusScript agents** or select **Edit** and click the drop-down arrow to display the contents of the Address Book.
4. Select the appropriate server, user, and/or groups, and click the **Add** button. Click **OK**. Close and save your changes to the Address Book.

   Note: The error message, "*Error validating user's agent execution access*" may indicate that an inappropriate Notes user or group was specified for **Run unrestricted LotusScript agents**.

Setting up an internet password

To securely access ScanMail from a Web browser, you should set up an Internet password. ScanMail uses Notes' own password scheme for restricting database access.

To set up Notes Internet passwords, open the Address Book and choose the **Person** you will grant access to. Enter a password in the **Internet password** field, then close and save your changes. (For additional information regarding Internet passwords, please consult your Notes documentation.)

Loading the HTTP task for web access

You must load the HTTP task to enable Web access to the ScanMail console. To load the task, go to the Notes server console and type **load http**. If you would like the HTTP task loaded each time you start ScanMail, edit `notes.ini` and add HTTP to the Server Tasks line. For example:

```
ServerTasks=tmmscan,repscan,router,HTTP...
```

Note: ***`Tmmscan`*** and ***`repscan`*** should be the first tasks that run before the Router starts mail delivery.

Enabling Relay Mail Scan in R4

Support for scanning out bound POP3 and SMTP traffic occurs automatically in Notes R5, but if you are running Notes R4, you will need to explicitly enable **Relay Mail Scan**.

To enable relay scanning on a Notes R4 server:

1. Create a new Notes mail user in your Name & Address book, for example, "SMLNrelay".
2. Add two new entries in the `notes.ini` file, which is usually located in the \WINNT directory:
   a. `SMRelay_User={SMLNrelay}/TrendMicro`

      (where the user is either the short or long name you created in Step 1)

   b. `SMInternet_Localdomain=trendmicro.com`

      For example: SMInternet_Localdomain=trendmicro.com, trendmicro.de, trendmicro.com.tw

      Note: If you have multiple Internet domains configured, use a comma for the delimiter. The maximum number of domain names is limited to five.

3. Restart the Notes server.

Disabling Relay Scanning

To disable Relay Scanning:

1. Stop the Notes server.
2. Remove the SMRelay_User and SMInternet_Localdomain lines from your `notes.ini` file.

Additional ways to update the virus pattern file

The virus pattern database can be updated manually, by downloading the file from the Web and copying it to the ScanMail directory, manually, by running the command "`pupdate`" in the Note command window, automatically, via active update server, and automatically, via Notes replication.

Updating via database replication

If you would like to obtain the pattern file via replication, configure replication from a server that has already obtained the latest virus pattern file via an Internet update or a replication from another server. To update the pattern file via replication, you no longer have to create a Server Program Update document because an event-driven agent executes whenever the pattern file is updated in the pattern database, `smency.nsf`.

Setting up rights for the "AutoDetachPattern" agent

When updating through replication, a Notes Agent detaches the file from the smency.nsf database under the data directory of the local server. This "AutoDetachPattern" Agent is an event-driven Agent, which is executed after changes in smency.nsf occur. It supersedes the pupdate program document configuration on every ScanMail server for pattern updates.

Note: Be sure that the ID being used has been assigned rights to run Agents.

To update the pattern file using the AutoDetachPattern Agent:

1. Replicate the `smency.nsf` database from another ScanMail server that has the latest pattern file attached.

2. Be sure to sign the `smency.nsf` database on both servers.
3. Add the server and the user who signed the database to the Run Unrestricted LotusScript/Java agents list.

Updating manually

Although the recommend practice is to schedule ScanMail to automatically update the virus pattern file and scan engine no less often than once a week, you can perform the updates manually by copying the files to the Notes data directory:

To update the virus pattern file:

1. Open a Web browser to the following URL:
   `http://www.trendmicro.com/download`
2. Choose ScanMail for Lotus Notes from the list of products that appears, and then scroll down the page that opens to find the **Virus Pattern File** for ScanMail.
3. Click the type of ScanMail you will be updating (Windows, OS-390/ and AS/400 or Unix) to begin downloading the compressed file to your local machine.
4. Extract and copy all files in the archive to the Notes data directory.

   The updated pattern file is automatically used for both real-time and manual scanning—you don't need to stop and restart the ScanMail scan tasks.

Note: We recommend that you keep the 1 or 2 most recent versions of the pattern file available for when you need to perform a "roll-back". You can delete all other pattern files in the directory (or schedule ScanMail to do it automatically).

Updating the scan engine

From the same web page, you can download scan engine updates (if any).

1. After making sure no scheduled ScanMail tasks are running, shut down both the real-time and database scan tasks by opening a Notes console and typing the following:

```
tell tmmscan quit
tell repscan quit
```

2. While the services are shutting down, return to the Web page you opened and scroll down to the **Scan Engines** section. Click the Scan Engine update that is appropriate for the ScanMail platform you are running to begin downloading.
3. Extract all files in the downloaded file to the Notes directory.
4. Restart the real-time email and database scan tasks as follows:

   ```
   load tmmscan
   load repscan
   ```

   The updated scan engine is automatically used for real-time email and database scanning, as well as for manual and scheduled scans.

Modifying the scan task's check-pattern interval

You can control how often the two ScanMail scan tasks, *tmmscan* and *repscan* check to see if the virus pattern file they are using is current, or if ScanMail has downloaded an more recent one from Trend Micro.

The default interval, 30 minutes, is fine for all but the heaviest server traffic. If you do have a situation where both *tmmscan* and *repscan* are almost continuously engaged in scanning, consider doubling or tripling the check-pattern interval.

To modify the interval check-pattern interval:

1. Open the notes.ini file in a text editor and then find or create the following line:

   ```
   SMPatternCheck_Interval=
   ```

2. Specify the number of minutes you the interval to be. The default is 30.

Chapter 4

Performing Real-time Email Scans

ScanMail’s real-time email scanning capabilities for Lotus Notes ensure that all email transactions are scanned: messages to and from individual Notes clients, as well as messages to and from a Notes client and people outside the Notes network. ScanMail for Lotus Notes also provides the option to protect against the latest security threat by scanning email hotspots for malicious code strings called "script bombs".

Mail scan allows you to take different actions for different threat types (quarantine viruses, delete script bombs, etc.), as well as allow you to customize threat-specific notification messages. In addition, you can use rich text for your virus notification messages. Separate internal and external notification messages can be configured in the warning to the sender and recipient(s).

The Attachment Blocking feature is particularly useful during virus outbreaks and enables configuration of a recipient exclusion list, which can help refine the block rules in order to allow exceptions.

The emergency outbreak mail delay option allows email to be held in a queue until filtering procedures or pattern/engine updates have been completed. This removes the need for the mail server to be shut down in case of a virus outbreak.

In this chapter you will find complete instructions for configuring real-time email scanning, including the following topics:

- Selecting the email attachments to scan in real time
- Configuring the scan options, such as stripping macros from Microsoft Office (Office) documents, scanning and cleaning compressed files, and scanning embedded objects
- Configuring the action on viruses found, including the new option to block an email message completely
- Entering regular text or rich text notification messages to the administrator(s), sender, and/or recipient(s) for viruses found
- Configuring the action and notifications for file attachments blocked and script bombs found
- Enabling customizable "Safe Stamps", "Encryption Stamps", Office macro strip notification, and ScanMail Disclaimer messages in scanned documents
- Configuring whether to save a copy of infected documents and/or a log of infected documents in the Quarantine database
- Setting up "Trusted Servers"
- Entering code strings and URLs to be checked in hotspot scanning
- Shutting down all instances of `tmmscan` that are running

Enabling/disabling email scanning

The ScanMail mail scan task starts automatically when Notes is launched.

Since ScanMail monitors all email passing to and from MAIL.BOX, it saves time and system resources by checking email before it is routed to the recipient(s). In this way, for example, an email addressed to 12 people that contains an infected attachment is scanned and cleaned once, on its way out from the sender, rather than 12 times, as it arrives in each of the recipients' mailboxes.

To temporarily stop or start mail scanning:

1. From the main ScanMail menu, click **Scan Options > Mail Scan**.

2. Under **Scan Options**, select **Enabled** or **Disabled**, depending on your needs. In the action bar above, click **Save & Exit**.

Configuring delivery of mail when ScanMail is not running

By default, the delivery of mail messages is not interrupted when scanning is stopped—the mail is just sent to the recipient without scanning. This parameter can be controlled in the `notes.ini` file:

`SMStopMail = 0` —mail is delivered without scanning

`SMStopMail = 1` —mail is held until scanning is restarted

Use the second option, for example, if you are waiting for a new pattern file during a virus outbreak.

While you do not need to stop or restart any tasks for the new pattern file to take effect, stopping mail delivery temporarily during outbreaks can be convenient until you have cleaned your existing documents. After you have cleaned your existing environment and updated the pattern file, be sure to manually release any mail that is being held.

Stopping and starting the mail scan task

To stop the mail scan task:

- Open a Notes console and type in the following line

```
tell tmmscan quit
```

To start the mail scan task:

- Open a Notes console and type in the following line

```
load tmmscan
```

Customizing real-time scans of email and attachments

Any mail attachment on the local Notes server can be scanned for viruses. ScanMail mail scans can detect viruses in UUencode, BINHEX, and MIME encoded attachments, as well as in attachments using a wide variety of compression types.

From the main Notes Workspace, bring up the ScanMail configuration window by double-clicking the **ScanMail for Lotus Notes** database icon. Click **Scan Options > Mail Scan** in the left navigator pane to open the Mail Scan configuration screen.

Configuring files to scan and scan options

In addition to checking the content of a email message (for things like script bombs), ScanMail can check the email attachments for viruses.

To have configure which attachments ScanMail should check:

1. From the main ScanMail menu, click **Scan Options > Mail Scan**.
2. Under **Files to scan** choose to scan all, or selected types, of email attachments.
   - Choose **Scan all files** to have ScanMail check every email attachment for viruses.
     - **Exclude files by true file type—**choose this option to omit certain file types from scanning. File type is determined by the internally registered type rather than by the file extension.
     - Exclude files by extension / name—choose this option to omit certain file types from scanning on the basis of the file extension (since the file name and extension are merely text labels, they can be changed arbitrarily and need not represent the actual file type).
   - Choose **Scan Selected files** to have ScanMail check only the file types you specify. By default, ScanMail suggests the file types below. Add or remove from this list to meet your needs.

```
*.ARJ, *.BAT, *.BIN, *.BOO, *.CAB, *.CHM,  *.CLA, *.CLASS,
*.COM, *.CSC, *.DAT, *.DLL, *.DOC, *.DOT,  *.DRV, *.EML,
*.EXE, *.GZ,  *.HLP, *.HTA, *.HTM, *.HTML, *.INI, *.JAR,
*.JS,  *.JSE, *.LNK, *.LZH, *.MDB, *.MPD,  *.MPP, *.MPT,
*.MSG, *.MSO, *.NWS, *.OCX, *.OFT, *.OVL,  *.PDF, *.PHP,
*.PIF, *.PL,  *.POT, *.PPS, *.PPT, *.PRC,  *.RAR, *.REG,
*.RTF, *.SCR, *.SHS, *.SYS, *.TAR, *.V,    *.VBE, *.VBS,
*.VSD, *.VSS, *.VST, *.WML, *.WSF, *.XD,   *.XLA, *.XLS,
*.XLT, *.XML, *.Z,   *.ZIP
```

Note: Scanning all files is marginally more secure than scanning only the Trend Micro recommendations. However, scanning all files can be expected to consume more system resources and take an increased amount of time. .

Selecting the scan options

After you have selected the files to scan, select the scan options to apply during the scan process:

- **Scan compressed files** — scans attachments that have been compressed using a wide variety of compression formats.
- **Clean compressed files** — enables cleaning of compressed files of types PKZIP, ZIP to EXE, LHA, and AMG. The file is decompressed to one layer for cleaning. If an infected file is found more than one layer down, the entire compressed file is marked as uncleanable.

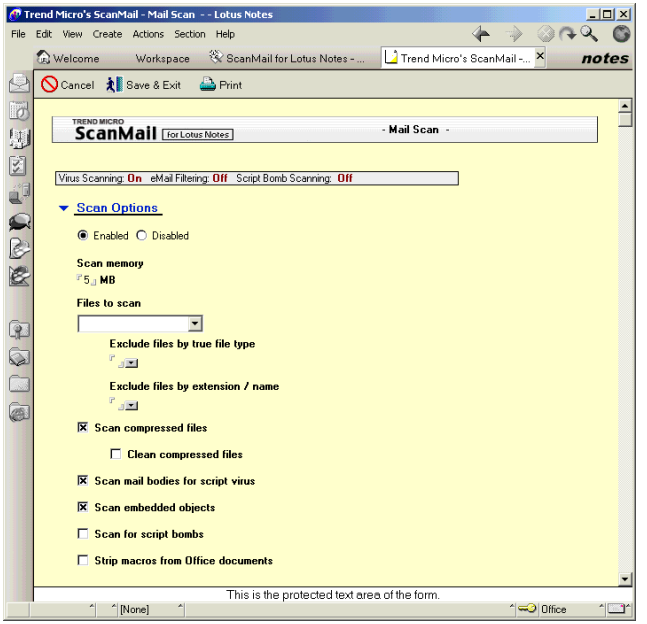


FIGURE 4-1. You can enable/disable real-time email scanning, and choose scan options.

Note: Compressed files can be cleaned only if all files contained are cleanable. If not, the entire compressed file is marked as uncleanable.

- **Scan Mail Bodies for Script Viruses** — checks the message text itself for known script viruses ("code" that is written in the mail body and executes when the script is run).
- **Scan embedded objects** — scans Microsoft Office objects that have been embedded in documents, for example, OLE objects.
- **Scan for script bombs** — scans documents for malicious code that is known as a "script bomb". Malicious code is a security threat that can cause as much damage as computer viruses. After you enable script bomb scanning, you need to configure the script strings to scan for. Click the **Script Bomb Scan** button to go to the configuration screen.

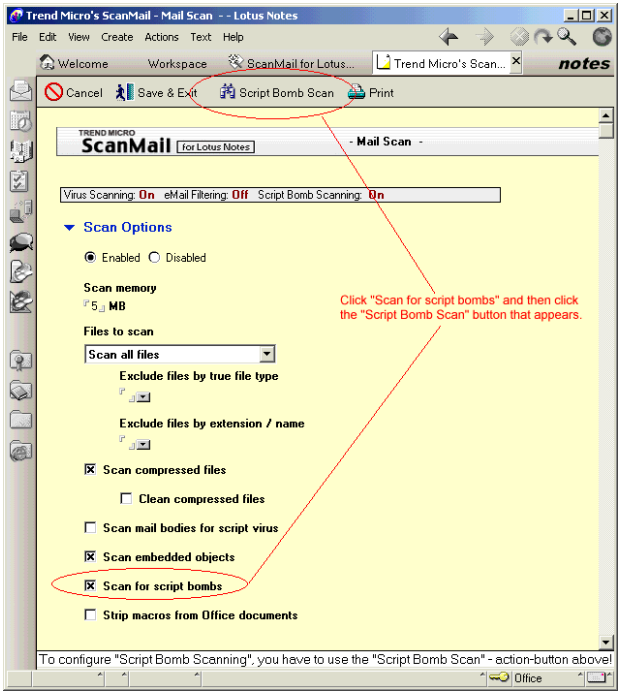


FIGURE 4-2. Scan email messages for so called "Script Bombs".

- **Strip macros from Office documents** — enables macros to be deleted from Office documents. Macros can contain malicious code that executes when the user opens a document and agrees to let the macros run.

Script scanning > Stored Form Scanning

Select the **Stored Form Scanning** check box. For a stored form hotspot containing malicious code or URLs (specified in the Scan String Lists section below), you can specify one of three actions for ScanMail to perform:

- Choose **Pass** to leave the stored form hotspot as it is *without cleaning*
- Choose **Delete** to remove the stored form from the database
- Choose **Auto Clean** to have ScanMail automatically clean stored form hotspots

Script bomb scanning

Lotus Notes scripts can contain malicious code. ScanMail can scan email body for these scripts.

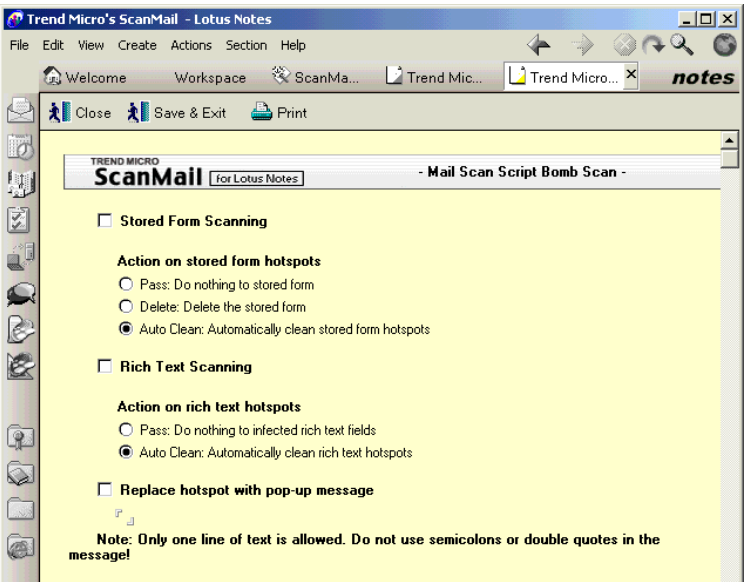


FIGURE 4-3. Enable stored form scanning, rich text scanning and disable hotspots.

By default, script scanning is not enabled on the Notes client.

To enable Script Bomb Scanning:

1. With the **Mail Scan** screen open, select the **Scan for script bombs** check box under **Scan Options**. The Script Bomb Scan button appears at the top of the screen.
2. Click the **Script Bomb Scan** button to open the **Mail Scan Script Bomb Scan** configuration screen.

Rich Text Scanning

Select the **Rich Text Scanning** check box. For a rich text hotspot containing malicious code or URLs (specified in the Scan String Lists section below), you can specify one of two actions for ScanMail to take:

- Choose **Pass** to leave the rich text hotspot as it is, *without cleaning*
- Choose **Auto Clean** to have ScanMail automatically clean rich text hotspots

Warning message

You can enter a hotspot warning message of your choice in the text field under **Replace hotspot with pop-up message**. For example, "ScanMail has detected a script bomb in this hotspot." If you do not wish to use a pop-up message, leave this field blank.

Note: Only one line of text is allowed for the hotspot message, which is 199 characters in single-byte environments or half of that for double-byte environments. Semicolons and double quotes are not supported.

Scan string lists

ScanMail provides Stored Form and Rich Text hotspot scanning based on user-definable strings contained in the following:

@Function strings can contain any valid Lotus Notes function. For example:

```
prompt
```

@Command strings can contain any valid Lotus Notes command. For example:

```
[execute], [FileDatabaseDelete]
```

Script strings can contain any valid script command from your operating system. For example:

```
shell, getobject, kill, mkdir, or activate
```

URLs called by @URLOPEN can contain any valid @URLOPEN command. For example:

```
offensivesite.com or www.offensivesite.com.
```

Additional Notification Message

To enable the administrator(s) to receive an additional notification message to emphasize that a virus was found during script bomb scanning, enter the text under **Additional Notification Message**.

Note: If the **Disable notification when viruses are cleaned** option is selected on the main Mail Scan Configuration screen, the additional notification message will not be sent either.

Use ScanMail's default alert message, or compose one of your own. To compose the message you want the administrator(s), sender, or recipient(s) to receive, type your message in the associated text field. For example,

Administrator: ScanMail for Lotus Notes has detected a possible script bomb.

This message is automatically sent to the person(s) indicated whenever ScanMail detects a script bomb.

Note: Each of these additional messages will be sent only when the related configuration choice is selected on the main Mail Scan Configuration screen.

You can fill in the **Add warning to original email** section to have the warning message to the recipient attached to the original email rather than sent as a separate message. Type in a text message for **Email subject** and/or **Email body.** By default, a warning will not be inserted in the original email message. If you select this option and also configure the **Warning to recipient** message, the recipient will get an additional notification message.

Working with trusted servers

ScanMail supports "trusted servers" -- any mail relayed from a trusted server will be added to the mail.box queue directly, without scanning. This feature is especially useful when the SMTP or Domino server feeding mail to ScanMail is also running antivirus software and there is no need to spend time scanning it twice.

To designate one or more servers as "trusted" servers:

1. In the **Mail Scan** page, open the **Scan Options** section and scroll down to Trusted servers.
2. Select the **Trusted AV Servers** check box, and then identify the server(s) you want ScanMail to trust. For SMTP servers, enter either the server's host name or IP address. For Domino servers, click the drop-down and pick from the list of servers that appears. Delimit multiple servers using a semi-colon. Wildcards are not valid for the server or organizational unit.

   Note: Only trust a **SMTP server** if it is running antivirus software such as ScanMail for Exchange or InterScan Messaging Security Suite, and the scanned mail is being relayed directly to the Domino server.

   Alternatively, you can identify the domino server by typing the fully qualified domain name (and country code, if any) in the text box. For example, `server1/OU1`.

Configuring an action on viruses

When ScanMail detects a virus in an email attachment, it acts only upon the infected file unless you choose the "Block" action (which blocks the entire message). The body of the email message and any uninfected files are sent to the original recipient.

You can specify one of five actions for ScanMail to take on the infected file:

Action on cleanable files

- **Pass** sends the infected attachment to the intended recipient(s) *without cleaning*. You can configure a warning message to send to the recipients.
- **Quarantine** moves, without cleaning, the infected email file to the quarantine database.

The intended recipient(s) will not receive the infected file. However, it does remain on the Notes server in the quarantine database. Depending on how you have it configured, the sender, the intended recipient, both, or neither are notified.

- **Delete** removes the infected file from the email and delete it from the server. The original message text of the email and any uninfected files are delivered to the intended recipient.
- **Block** blocks infected files from delivery. The entire email message is blocked from delivery, including the text, header, and all attachments.
- **Auto Clean** cleans infected files and then sends them to the intended recipient(s). This is the default recommended action so that cleaned mail is delivered.

Action on uncleanable files

In some cases due to the nature of the virus, it can be identified but cannot be cleaned. For example, the EICAR test virus was created as an uncleanable virus. When the virus cannot be cleaned, you can have ScanMail delete the infected attachment, move it to the quarantine database, pass it along without cleaning, or block the entire message completely.

Note: If uncleanable files are found within a compressed attachment, the compressed attachment is marked as uncleanable. The entire compressed attachment is passed, quarantined, blocked, or deleted as configured. The body of the email message and any other uninfected attachments are sent to the original recipient(s).

Action on special virus types

Although ScanMail is able to detect malicious, non-virus threats such as the mass-mailers, worms, Trojans, jokes, zip-of death, and a host of other threats, because these programs are not, strictly speaking, viruses, they cannot be cleaned.

Action on unscannable files

In addition to viruses and non-virus threats, another potentially dangerous category exists: messages that cannot themselves be opened, or they contain attachments that cannot be opened for example because the attachment is password-protected, encrypted, or corrupted.

You may also want ScanMail to act on messages that present certain unseemly characteristics such as compressed files that extract hundreds of megabytes upon extraction, or compressed files that contain 20, 30, even 40 layers. Files such as these are often intended to crash the mail server by occupying all free space or CPU.

Whenever ScanMail comes across files that cannot be read, it performs one of the following actions: **Quarantine**, **Delete**, **Block**, or **Pass**.

Whenever ScanMail detects a *non-virus threat* that cannot be cleaned, it performs one of the following actions: **Quarantine**, **Delete**, **Block**, or **Pass**. The event is recorded in the logs, warnings are sent, and the message is delivered to the recipient.

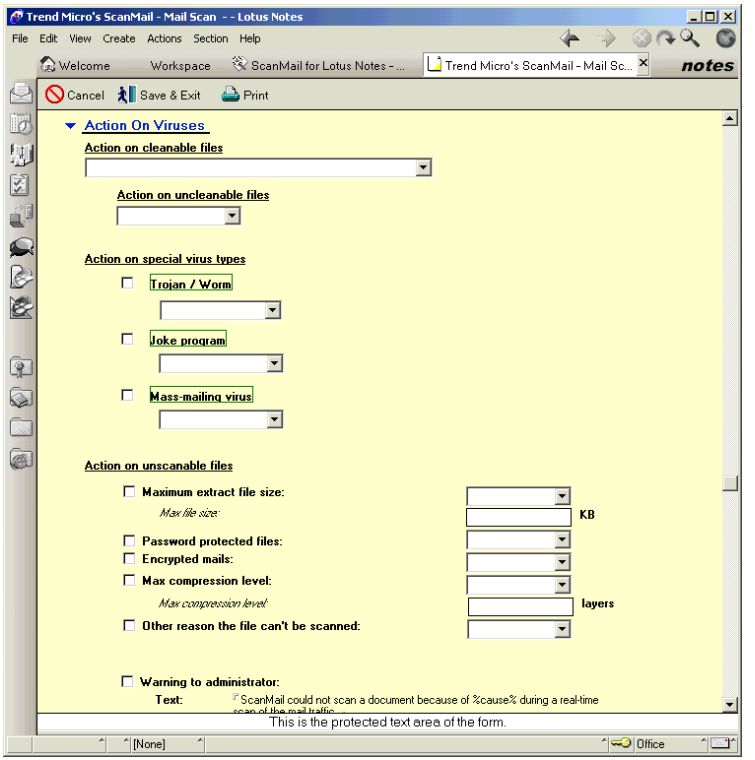


FIGURE 4-4. In addition to viruses, ScanMail detects non-virus threats such as worms, Trojans, jokes, and inaccessible files (encrypted or password-protected, which cannot be cleaned).

Configuring virus notification

When a virus is discovered in an email attachment, ScanMail can automatically alert, via email, the people you designate—for example, the Notes administrator or other individuals who need to know when infected files are found, the sender, and/or the recipient(s).

In the case of the administrator, the alert is sent as a separate email, whereas for the recipient, it is appended to the original email that contained the infected file. In addition to the notification message, ScanMail includes details about the virus, such as the name of the infected database, the virus name, and the action ScanMail took. This information is also archived in ScanMail's log files.

When no viruses are found, you can have ScanMail append a "Safe Stamp" message telling users their email was scanned and found to be virus-free.

Setting the notification message return address

Notes uses the server name as the default name for program notification messages. You can select an administrator's name as the default so that notifications will be sent to a particular user rather than the server ID.

Click the drop-down arrow and select the Administrator you would like set as the default. All replies to ScanMail messages will be sent to this account.

In all configurations, you can use ScanMail's default message or compose one of your own. You can choose to send plain text ScanMail notification messages or use the new rich text format. Rich text format is used to customize the background, graphics, and text style for the notifications.

Regular Text Notification

While not as elegant as rich text, plain text notification messages contain all the necessary information to inform administrator(s), sender, and recipient(s) of virus detections.

To enable regular text notifications:

1. Make sure the **Enable rich text notification** check box is not selected.
2. Select **Warning to administrators** to have ScanMail automatically alert the Notes Administrator or other individuals who need to know when infected files are found.

a. In the **Administrator(s)** field, type the email address of the person you want notified. ScanMail can send the alert to more than one person. Use a comma as the delimiter between addresses.

Alternatively, you can click the drop-down arrow and select from the list of names that appears. Any address in the public & personal address books is eligible for this notification, including SMTP addresses.

b. To compose the message you want the Administrator (and anyone else) to receive, type your message in the associated **Text** field. For example,

Administrator: ScanMail has detected a virus during a real-time scan of the email traffic.

Note: ScanMail supports multiple line notification messages. Press the "Enter" key at the end of each line.

This message is automatically sent to the person or persons indicated in the **Warning to** field whenever ScanMail detects a virus.

3. Select **Disable notification when viruses are cleaned** to omit notification to the Administrator when viruses have been scanned and cleaned.

For example, if you have experienced many Word macro viruses and do not need to be notified when every infected macro is deleted, this selection could save you many additional notification messages.

4. Select **Warning to sender** and/or **Warning to recipient(s)** to warn either sender or recipients or both when a virus is found, put a check in the appropriate box(es). Enter the message you want that person to receive in the associated **Text** fields. These message is sent as a separate email. **Internal** refers to messages sent within your primary address book, whereas the **External** message is sent to users outside the network and in secondary address books.

Note: In addition to the message text, ScanMail also includes in its email to the recipient the **date** the file was sent, the **sender's name** and email address, the name of the **infected file**, the **virus name**, and the **action** ScanMail took on the file. These notifications are not user-configurable.

---

5. **Add warning to the original email if a virus is detected** can be configured to insert warnings into recipient's original email message when infected

attachments are detected. Enter the text message that you would like included in the **Mail Subject**. Select the check box **Add virus information to mail** if you would like to include virus details in the mail body.

If you select this option and also configure the **Warning to recipient(s)** message, the recipient receives an additional notification message.

Rich text notification

Use rich text format if you want to add formatting to your text messages. Rich text is currently supported through the ScanMail Notes client interface (i.e., not the ScanMail Web browser interface).

To enable rich text notification:

1. Select **Enable rich text notification**.
2. Click **Update rich text notification** to go to the rich text configuration screen.
   a. Fill in the **Subject** with a text message.
   b. If you are using the Notes client, create the rich text notification message you would like sent in the subject body.

      -or-

      If you are using a Web Browser, click **Browse** to locate the file name that you would like to include as rich text.
   c. Click **Save & Exit.**
3. Select **Warning to administrators** to have ScanMail automatically alert the Notes Administrator or other individuals who need to know when infected files are found.

4. In the **Administrator(s)** field, type the email address of the person you want notified. Alternatively, you can click the drop-down arrow and select from the list of names that appears.

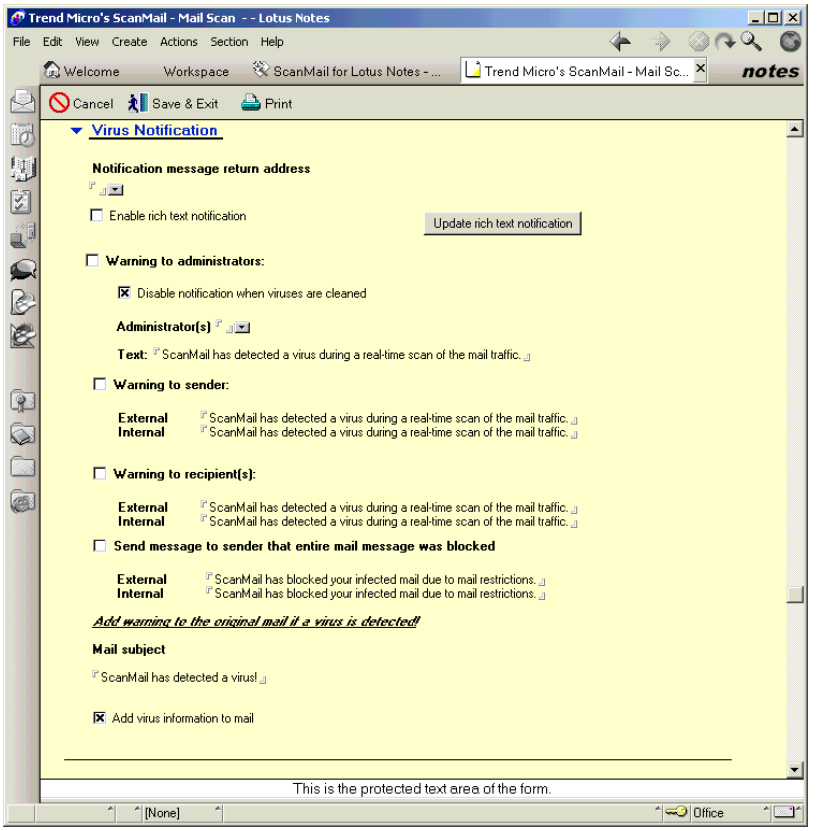


FIGURE 4-5. Mail Configuration screen, Virus Notification section, (regular text notification shown here).

5. Select **Disable notification when viruses are cleaned** to omit notification to the administrator when viruses have been scanned and cleaned.
6. Select **Warning to sender** and/or **Warning to recipient(s)** if you would like the sender or recipient(s) notified via rich text.

Note: The same Rich Text notification message is sent to the administrator(s), sender, and recipient(s) selected. If you want to send Rich Text notification only, make sure that the Regular Text notification fields are empty.

7. **Add warning to the original email if a virus is detected** can be configured to insert warnings into recipient's original email message when infected attachments are detected. Enter the text message that you would like included in the **Email Subject**. Select the check box **Add virus information to mail body** if you would like to include virus details in the mail body.

Virus logging options

The Virus Logging options are not selected by default. Select the check box(es) if you would like to enable these options.

- **Save a copy of infected documents in the Quarantine database** — if you do not save a copy of infected documents, they will be deleted from your system. When you enable this option, a full copy of infected documents is saved in `\data\smquar.nsf`.
- **Keep a log and a copy of encrypted documents in the Quarantine database** — if you would like to keep a log of which documents were encrypted and thus could not be scanned on the server (encrypted files cannot be opened except by the original intended recipient).

Email stamps

Email Stamps can be inserted into scanned messages to inform the recipient that mail has been scanned and does not contain viruses. Stamps can be used to indicate that mail is encrypted and can't be scanned or that a macro has been stripped from the message:

To enable email stamps, select one of more of the following check boxes:

- **Safe Stamp** — informs your users that their email was scanned and was found to be virus-free. Enter the text of the message you want ScanMail to send (regular text), for example:
  (ScanMail—safe message)

This message is appended to the subject field of the email when no viruses have been found. Leave the **Safe Stamp** option unchecked if you want ScanMail to operate invisibly in the background unless a virus has been found.

WARNING! *The Safe Stamp is added to a message when no viruses have been found. However, if you are not also scanning for Script Bombs, the email could still contain malicious content.*

- **Encrypted Stamp** — informs your email users that their encrypted email was not scanned on the server. Enter the text of the message you want ScanMail to send (regular text), for example,

  Encrypted: Not scanned.

  This message is appended to the subject field of the email when a message was not scanned due to encryption. Leave the **Encryption Stamp** option unchecked if you do not want to inform your users.

- **Office macro strip notification** — informs your email users that an office macro was stripped out of their message. Enter the text of the message you want your users to receive, for example:

  Office macro security is enabled. Office macro(s) have been stripped from this document.

- **Disclaimer** — inserts a disclaimer into mail that has been scanned. Enter the text of the message you want your users to receive.

eManager / filter rules

You can have ScanMail send out notification messages whenever an eManager filter rule finds a match. In addition, if you plan to use eManager's email filtering, you will need to be sure **eMail filtering** is enabled in the Mail Scan page.

WARNING! After creating Filter Rules and/or Content Filters , you must enable eMail filtering in the Mail Scan screen for the rule to be enacted.

To enable email filtering:

1. At the main ScanMail menu, choose **Mail Scan**, scroll to the bottom of the page, and open the **eManager / Filter Rules** option.

2. Double-check to be sure **eMail Filtering** is **Enabled**, and confirm that your current Filter Rule appears in the list of Active Filter Rules.
3. On the same page, after customizing the notification options, etc. click **Save & Exit** to apply the filter.

Specifying the temporary directory

Unless you specify otherwise, ScanMail creates and uses the following temporary directory to use for mail scanning:

```
\Lotus\Domino\Data\smln\SMTemp\MailTemp\
```

If you would like to specify a different temporary directory to use, you can change the default.

You need to stop and restart the Mail Scanner task before the new temporary directory will be used. To restart the mail scanner, at the server console type

```
tell tmmscan quit
```

and then

```
load tmmscan
```

Saving the mail configuration

To save the new configuration, click **Save & Exit** (Notes client) or **Save** (Web browser), located at the top of the screen. To cancel your changes and revert to the last saved configuration, click **Cancel**.

You do not need to restart the Notes server for the configuration changes to take effect. All email sent and received will now be scanned according to your new configuration settings.

Chapter 5

Performing Real-time Database/Replication Scans

An important part of maintaining a virus-free Notes environment is ensuring that viruses are not spread during real-time database access and replication. To minimize this risk, we recommend that you install a copy of ScanMail on each of the Notes servers in your organization, perform a Manual scan of all databases to check for viruses, then start the real-time database scanning task.

Replication scanning can be an intensive operation when many large databases are involved. ScanMail is designed to maximize both efficiency and security by checking and cleaning a document on the server that ScanMail is installed on *as* it is saved, *before* it is replicated to other Notes servers or clients.

ScanMail for Lotus Notes also provides the option to protect against the latest security threats by scanning document hotspots for malicious code strings called "script bombs". Real-time database scans provide separate treatment and notification options for virus-infected documents and script bombs found.

ScanMail for Lotus Notes supports memory-based scanning, which significantly increases scanning speed. In addition, it contains options to strip macros from Office documents and scan embedded OLE objects.

Complete instructions for configuring the real-time database and replication scanning are detailed in this chapter, including the following topics:

- Configuring the file attachments to scan in real time
- Selecting the scan options, such as stripping office macros from documents, scanning and cleaning compressed files, and scanning embedded objects
- Selecting the databases to include for scanning or exclude from scanning
- Configuring the action on viruses and script bombs found
- Entering notification messages to the administrator(s) for viruses and script bombs found
- Configuring whether to save a copy of infected documents and/or a log of infected documents in the Quarantine database
- Entering code strings and URLs to be checked in script scanning

Real-time database scan configuration screens

ScanMail for Lotus Notes has two Real-time Database configuration screens:

1. **Main configuration**—where you can select the databases to scan as well as configure Scan Options, Actions, Notifications, and other related tasks.
2. **Script Scan**—configure Stored Form Hotspot and Rich Text Hotspot scanning.

Which file attachments can be scanned in real time?

Real-time database scanning can be time-consuming when it involves many databases, each containing thousands of frequently updated documents. As such, it is advisable to activate real-time scanning only for those databases most likely to become infected—specific user databases, for example, rather than Lotus's native Notes databases. For these, you can always perform database scans of the local hard drive if you like.

Scanning notes databases replications in real-time

From the main Notes Workspace, access the ScanMail configuration window by double-clicking the **ScanMail for Lotus Notes** database icon. You can access the

Real-time Scan configuration by choosing **Scan Options >Real-time Scan** in the left navigator pane.

Enabling/disabling real-time scans

The ScanMail replication scan task starts automatically when Notes Domino server is launched. With real-time scanning enabled, ScanMail monitors data replications and all read/write activity to the database. For example, if a user posts to a central Notes database an Office document that contains a macro virus, ScanMail detects the virus before the document is ever added to the database.

Likewise, if replication is schedule between two databases, ScanMail monitors the replication and detects any viruses that may be buried in the database.

To temporarily stop or start real-time database scanning:

1. From the main ScanMail menu, click **Scan Options > Real-time Scan**.
2. Under **Scan Options**, select **Enabled** or **Disabled**, depending on your needs. In the action bar above, click **Save & Exit**.

Configuring files to scan and scan options

Under **Files to scan** you can choose to scan all email attachments, or only certain types for scanning.

- Choose **All attached files** to have ScanMail check every email attachment for viruses. This is the most secure option.
- Choose **Scan Selected** files to have ScanMail check only the file types you specify. By default, when you select this option ScanMail suggests about 60 recommended files types. You can accept this default, or add and remove extensions at your discretion:

  *.ARJ, *.BAT, *.BIN, *.BOO, *.CAB, *.CHM, *.CLA, *.CLASS, *.COM, *.CSC, *.DAT, *.DLL, *.DOC, *.DOT, *.DRV, *.EML, *.EXE, *.GZ, *.HLP, *.HTA, *.HTM, *.HTML, *.INI, *.JAR, *.JS, *.JSE, *.LNK, *.LZH, *.MDB, *.MPD, *.MPP, *.MPT, *.MSG, *.MSO, *.NWS, *.OCX, *.OFT, *.OVL, *.PDF, *.PHP, *.PIF, *.PL, *.POT, *.PPS, *.PPT, *.PRC, *.RAR, *.REG, *.RTF, *.SCR, *.SHS, *.SYS, *.TAR, *.V, *.VBE, *.VBS, *.VSD, *.VSS, *.VST, *.WML, *.WSF, *.XD, *.XLA, *.XLS, *.XLT, *.XML, *.Z, *.ZIP

Selecting the Scan Options

After you have selected the files to scan, select the scan options to apply during the scan process:

- **Scan compressed files** — scans attachments that have been compressed using a wide variety of compression formats.
- **Clean compressed files** — enables cleaning of compressed files of types PKZIP, ZIP to EXE, LHA, and AMG. The file is decompressed to one layer for cleaning. If an infected file is found more than one layer down, the entire compressed file is marked as uncleanable.

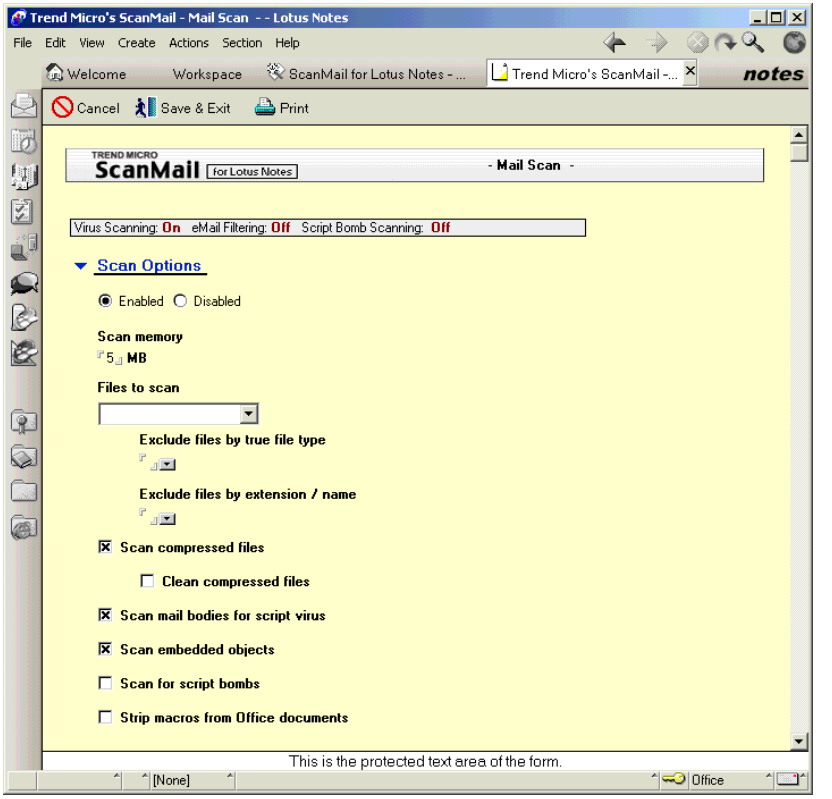


FIGURE 5-1. You can enable/disable real-time scanning and choose the scan options.

Note: Compressed files can be cleaned only if all files contained are cleanable. If not, the entire compressed file is marked as uncleanable.

- **Scan Mail Bodies for Script Viruses**— checks the message text itself for known script viruses ("code" that is written in the mail body and executes when the script is run).
- **Scan embedded objects** — scans Microsoft Office objects that have been embedded in documents, for example, OLE objects.

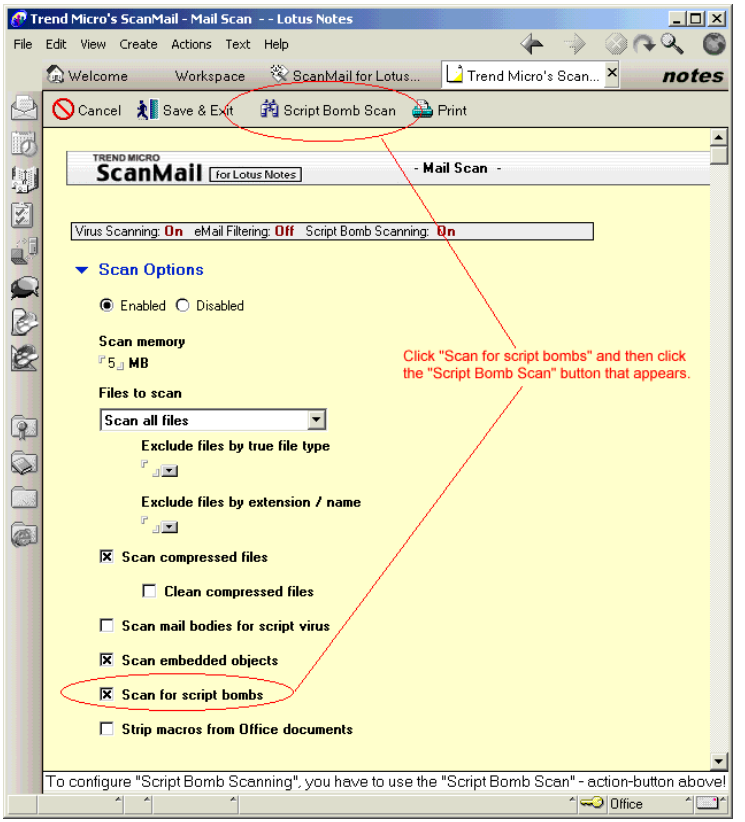


FIGURE 5-2. You can scan email messages for so called "Script Bombs".

- **Strip macros from Office documents** — enables macros to be deleted from Office documents. Macros can contain malicious code that executes when the user opens a document and agrees to let the macros run.

Stored form scanning

Select the **Stored Form Scanning** check box. For a stored form hotspot containing malicious code or URLs (specified in the Scan String Lists section below), you can specify one of three actions for ScanMail to take:

- Choose **Pass** to leave the stored form hotspot as it is *without cleaning*
- Choose **Delete** to remove the stored form hotspot from the database
- Choose **Auto Clean** to have ScanMail automatically clean stored form hotspots

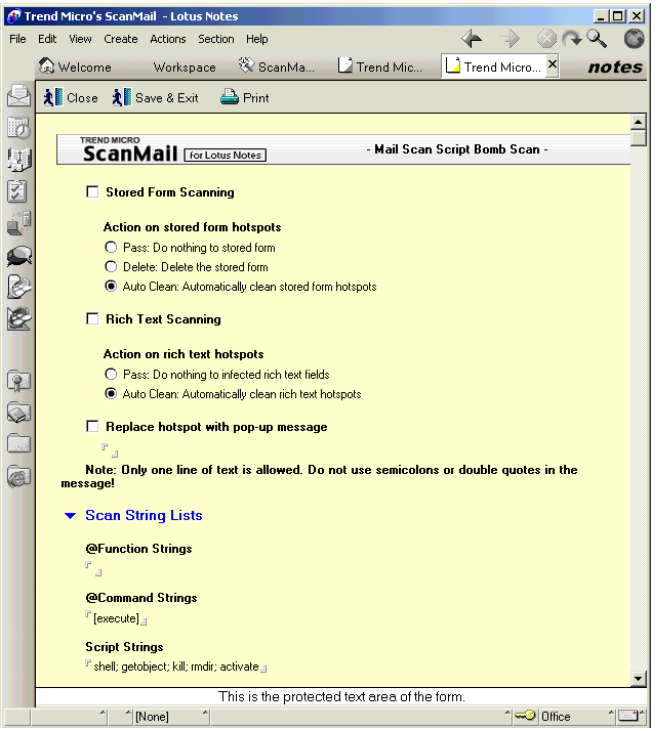


FIGURE 5-3. You can enable stored form and rich text scanning and disable hotspots.

Rich Text Scanning

Select the **Rich Text Scanning** check box. For a rich text hotspot containing malicious code or URLs (specified in the Scan String Lists section below), you can specify one of two actions for ScanMail to take:

- Choose **Pass** to leave the rich text hotspot as it is, *without cleaning*
- Choose **Auto Clean** to have ScanMail automatically clean rich text hotspots

Warning message

You can enter a hotspot warning message of your choice in the text field under **Replace hotspot with pop-up message**. For example, "ScanMail has detected a script bomb in this hotspot." If you do not wish to use a pop-up message, leave this field blank.

Note: Only one line of text is allowed for the hotspot message, which is 199 characters in single-byte environments or half of that for double-byte environments. Semicolons and double quotes are not supported.

Scan string lists

ScanMail provides Stored Form and Rich Text hotspot scanning based on user-definable strings contained in the following:

@Function strings can contain any valid Lotus Notes function. For example:

```
prompt
```

@Command strings can contain any valid Lotus Notes command. For example:

```
[execute], [FileDatabaseDelete]
```

Script strings can contain any valid script command from your operating system. For example:

```
shell, getobject, kill, mkdir, or activate
```

URLs called by @URLOPEN can contain any valid @URLOPEN command. For example:

```
offensivesite.com or www.offensivesite.com.
```

Additional notification message

To enable the administrator(s) to receive an additional notification message to emphasize that a virus was found during script bomb scanning, enter the text under **Additional Notification Message**.

Note: If the **Disable notification when viruses are cleaned** option is selected on the main Mail Scan Configuration screen, the additional notification message will not be sent either.

Use ScanMail's default alert message, or compose one of your own. To compose the message you want the administrator(s), sender, or recipient(s) to receive, type your message in the associated text field. For example,

Administrator: ScanMail for Lotus Notes has detected a possible script bomb.

This message is automatically sent to the person(s) indicated whenever ScanMail detects a script bomb.

Note: Each of these additional messages will be sent only when the related configuration choice is selected on the main Mail Scan Configuration screen.

Scanning selected databases

A good strategy for maximizing security while minimizing the demand on system resources is to designate only the highest risk databases for routine inclusion in real-time replication scanning. The rest can be scanned on the server using Manual or Scheduled database scanning, discussed in Chapter 6, "Performing Manual and Scheduled Scans."

Note: After you change the status of **Databases to Scan** (by including or excluding different files), you do not need to restart the Notes server.

To scan all databases in real time, select **All databases**. Alternatively, you have the option to include selected databases for scanning, or exclude selected databases. If you have only a few databases that you need to scan, you can specify them in an

inclusion list. If you have a large number of databases and need to exclude only a few from scanning, you can use an exclusion list instead.

To select databases for scanning from the Notes client console:

1. Click **Scan selected databases only**.
2. Click the **Add.**
3. From the list that appears, choose the databases you want scanned. Click a database to select it. You can select multiple databases at once. Click **OK**. (Directories cannot be selected for real-time scanning).

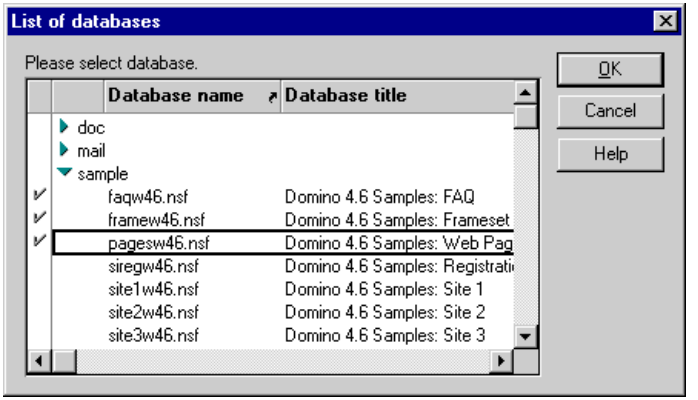


FIGURE 5-4. Scanning only selected databases saves time.

You'll notice that ScanMail runs a quick cleanup script called **Delete all db-documents** before adding the database. This script does not act upon your databases; instead it deletes a temporary list of documents that ScanMail created.

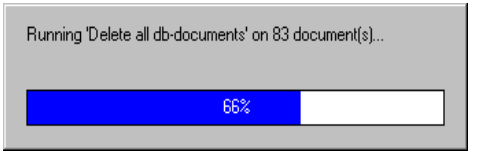


FIGURE 5-5. The ScanMail cleanup script creates this message on the Notes client console.

4. Click **Remove** to remove individual databases from the list that appears if you do not want them scanned or the **Remove All** button to remove all database names to be included.

Excluding Databases

Alternatively, you can choose to exclude selected databases from scanning.

To exclude databases from scanning on the Notes client console:

1. Click **Exclude selected databases from scanning**.
2. Click **Add**, and from the list that appears, choose the databases you want excluded from scanning. Click a database to select it. You can select multiple databases at once.
3. Click **OK**, them **Remove** to delete individual databases from the list that appears if you do not want to exclude them from scanning or the **Remove All** button to remove all database names to be excluded. Therefore, any databases removed from this list are scanned.

Configuring the action on viruses

When ScanMail detects a virus in an attached file contained in a document during replication, it acts only upon the infected file. The document's original rich text format and any uninfected files that were also attached are not affected.

For the infected file, you can specify one of four actions for ScanMail to perform:

- **Pass** leaves the infected file as is, without cleaning. A warning message including the text you specified is generated and sent to the designated administrator.
- **Quarantine** removes the infected file from the database and moves it, *without cleaning*, to the quarantine database.
- **Delete** removes the infected file from the database and delete it from the server. The original rich text format portion of the document and any uninfected attached files are left intact and replicated as normal. The Notes administrator and any others designated are sent a notification message via email.
- **Auto Clean** automatically cleans infected files.

Action on uncleanable files

In some cases due to the nature of the virus, it can be identified but cannot be cleaned. For example, the EICAR test virus was created as an uncleanable virus. When the virus cannot be cleaned, you can have ScanMail delete the infected attachment, move it to the quarantine database, pass it along without cleaning, or block the entire message completely.

Note: If uncleanable files are found within a compressed attachment, the compressed attachment is marked as uncleanable. The entire compressed attachment is passed, quarantined, blocked, or deleted as configured. The body of the email message and any other uninfected attachments are sent to the original recipient(s).

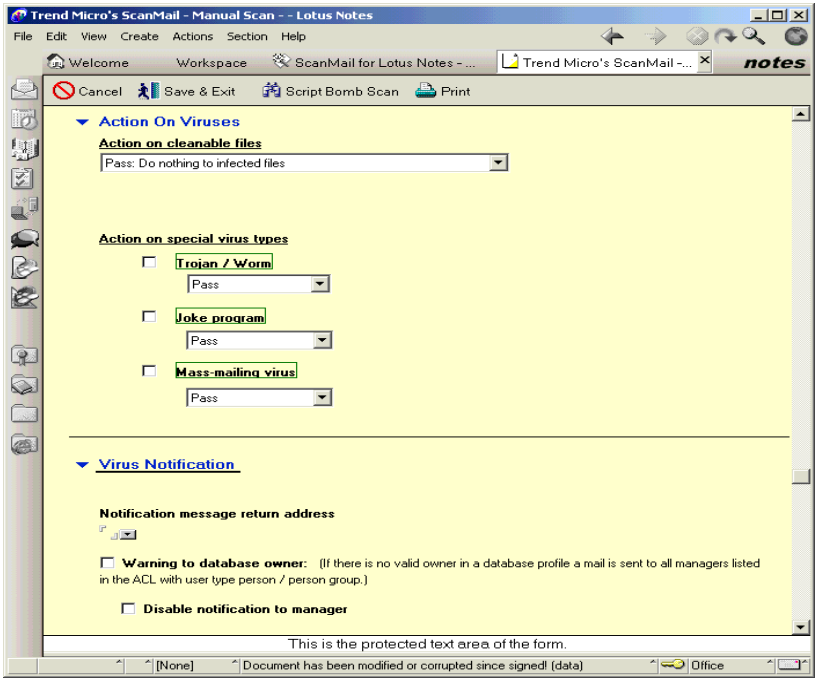


FIGURE 5-6. In addition to viruses, ScanMail detects non-virus threats such as worms, Trojans, and jokes. Since these files are not "infected", they cannot be cleaned.

Action on special virus types

Although ScanMail is able to detect malicious, non-virus threats such as the mass-mailers, worms, Trojans, jokes, zip-of death, and a host of other threats, because these programs are not, strictly speaking, viruses, they cannot be cleaned.

Whenever ScanMail detects a non-virus threat that cannot be cleaned, it performs one of the following actions: Quarantine, Delete, Block, or Pass (write the event to logs, send a warning, but deliver the message to the recipient as usual).

Configuring virus notification

When a virus is discovered during replication, ScanMail can automatically alert, via email, the people you designate—for example, the Notes administrator or other individuals who need to know when infected files are found. You can use ScanMail's default alert message, or compose one of your own. Additional details about the virus are also included, such as the name of the infected database, the virus name, and the action ScanMail took. This information is also archived in ScanMail's log file.

To have ScanMail automatically alert the Notes Administrator:

1. From the main ScanMail menu, click **Scan Options** > **Real-time Scan** and scroll down the Real-time Scan page that appears to the **Virus Notifications** section.
2. In the **Notification message return address** field, enter the email address that you want to appear in the **From:** field of the notification message that is sent.
3. Click **Warning to database owner** to have ScanMail automatically notify the person who is listed in the database profile as owner. (If this option is selected but no owner is found, ScanMail notifies all Managers unless this option is specifically disabled in the **Disable notification to manager** field.)
4. In the **Warning to administrator(s)** field, type the email addresses of the persons you want notified or select from the drop-down list.

Note: To specify multiple recipients, delimit addresses with a comma.

---

5. Next, type the message you want to send in the associated text field. For example,

   Administrator: ScanMail for Lotus Notes has detected a virus during a real-time database/replication scan.

In addition to the message text, ScanMail also includes in its email the **name** and **date** of the infected file, the **virus name**, and the **action** ScanMail performed on the file. These notifications are not user-configurable.

Virus logging options

The Virus Logging options are not selected by default. You can select any of the following options:

- **Save a copy of infected documents in Quarantine database** — if you do not save a copy of infected documents, they are deleted from your system. When you enable this option, a full copy of infected documents is saved in `\data\smquar.nsf`.
- **Keep a log of encrypted documents in Quarantine database** — select this option to log of encrypted documents that could not be scanned on the server (encrypted files cannot be opened except by the original intended recipient).

Specifying the temporary directory

Unless you specify otherwise, ScanMail will create and use the following temporary directory to use for real-time database scanning:

```
\Lotus\Domino\Data\smln\SMTemp\RepTemp\
```

To specify a different temporary directory to use, you can change the default.

Tip: Stop and restart the Real-time Database Scanner task before the new temporary directory is used.

Saving the new configuration

To save the new configuration, click the **Save & Exit** button (Notes client) or **Save** button (Web browser), located at the top of the screen. To cancel your changes and revert to the last saved configuration, click **Cancel**.

Chapter 6

Performing Manual and Scheduled Database Scans

ScanMail for Lotus Notes recognizes the unique file format of Notes databases. This allows it to open Notes databases and scan the individual documents, and any attached files, for viruses. One of the first things you should do after installing ScanMail is to run a Manual database scan of all the directories that contain Notes databases to find and clean any existing viruses. After performing the initial scan of all Notes databases, we recommend that you schedule ScanMail to automatically check Notes databases on the local or remote hard drives on a periodic basis.

You can enable "Incremental Scanning" for Manual and Scheduled Scans. Incremental scanning allows scanning of new and newly modified documents only, which can save considerable server CPU time and resources.

ScanMail for Lotus Notes also provides the option to protect against the latest security threat by scanning document Hot spot for malicious code strings called "script bombs". Manual and Scheduled database scans also provide separate treatment options for virus-infected documents and script bombs found.

ScanMail for Lotus Notes provides new options to include and/or exclude certain databases/directories from being scanned by Manual and Scheduled Scan. In addition, there are new options to strip macros from Microsoft Office documents and scan embedded OLE objects.

This chapter provides instructions for configuring Manual database scans. In addition, it covers how to configure ScanMail to perform Scheduled scans. The topics include:

- Configuring the file attachments to scan
- Selecting the scan options, such as stripping office macros from documents, scanning and cleaning compressed files, and scanning embedded objects
- Selecting the databases and/or directories to include or exclude from scanning
- Configuring the action on viruses and script bombs found
- Entering notification messages to the administrator(s) for viruses and script bombs found
- Configuring whether to save a copy of infected documents or log of infected documents in the Quarantine database
- Setting up Incremental Scanning to save server time and resources
- Entering code strings and URLs to be checked in script scanning
- Configuring ScanMail to automatically perform Scheduled scans
- Stopping all currently running scans with the command "load dbscan quit"

Database scan configuration screens

ScanMail for Lotus Notes has two database configuration screens for Manual and Scheduled database scans:

1. Main configuration—familiar from previous versions of ScanMail.
2. Script Scan — configure Stored Form Hotspot and Rich Text Hotspot scanning.

Customizing Manual and Scheduled database scans

Any database on the local Notes server, or remote clients with drives or directories mapped to the local server, can be scanned for viruses. Only Notes database files are eligible for Manual and Scheduled database scans.

Before performing a scan of your databases, specify what databases (or directories) to scan.

Note: If no databases or directories have been selected, ScanMail will have nothing to scan. we recommend to always check what you're scanning before saving the configuration.

The configuration choices are the same for Manual and Scheduled database scans. This chapter describes the choices you will see for either option. Under **Database Scan** in the left navigator pane, select either:

- Manual Scan
- Scheduled Scan

The screen for the option you chose appears. First we will describe the required fields that are common to both types of scans.

Configuring the files to scan and scan options

ScanMail scans the files attached to Notes documents for viruses, employing both Trend Micro's MacroTrap technology and its multi-threading 32-bit scan engine to detect macro, polymorphic, file, boot sector, and other viruses.

Under **Files to scan**, you have the following options:

- Click the **All attached files** radio button if you would like to have the most secure configuration, wherein every attached document is checked for viruses, regardless of its extension.
- If you would like to minimize real-time scanning, click the **Attached files with selected extensions** radio button, then click the drop-down arrow under **User-defined file extensions**. Choose the file names you want scanned by clicking on them.

  If you would like to define additional file names to include for scanning, enter the file types in the **New Keywords** text box, separated by semicolons. For example:

  ```
  prg; pgm
  ```

Selecting the scan options

After you have selected the files to scan, select the scan options to apply during the scan process:

- **Strip macros from Office documents** — enables macros to be deleted from Microsoft™ Office documents. Macros can contain malicious code that executes when the user opens a document and agrees to let the macros run.
- **Scan compressed files** — scans attachments that have been compressed using a wide variety of compression formats.
- **Clean compressed files** — enables cleaning of compressed files of types PKZIP, ZIP to EXE, LHA, and AMG. The file is decompressed to one layer for cleaning. If an infected file is found more than one layer down, the entire compressed file is marked as uncleanable.

Note: Compressed files can be cleaned only if all files contained are cleanable. If not, the entire compressed file is marked as uncleanable.

- **Scan for script bombs** — scans documents for malicious code that is known as a "script bomb". Malicious code is a security threat that can cause as much damage as computer viruses, if left unchecked. After you enable script bomb scanning, you need to configure the script strings to scan for. Click **Script Bomb Scan** to go to the configuration screen.
- **Scan embedded objects** — scans Microsoft Office objects that have been embedded in documents, for example, OLE objects.

Configuring databases and/or directories to scan

You can scan selected databases individually or by directory. Database scanning applies only to Notes databases. Other file types are not scanned by ScanMail for Lotus Notes. A good strategy for maximizing security while minimizing the demand on system resources is to scan your lowest risk Notes databases using a scheduled scan rather than scanning during replication. This is because the process of replication is already quite network intensive, and the added task of virus scanning and cleaning contributes to the load.

You can select any Notes database on the local hard drive or mapped network drives for scanning. For Manual and Scheduled Scans, you can specify the databases to scan individually or by directory.

Scanning selected databases

There are two ways to scan selected databases:

- Scanning directly from the Notes server command line
- Scanning using the ScanMail interface

Database scanning from the Notes server command line

From the Notes server command line, type in the following command followed by the name of the database you want scanned:

load dbscan yourdatabase.nsf

The Notes data directory is assumed unless you specify a different directory. Also, remember to delimit multiple databases with a space.

Stopping all instances of dbscan

You can stop all database scans from the Notes server command line by entering:

```
tell dbscan quit
```

This command stops all instances of dbscan that are running after the current document has been scanned.

Database scanning from the ScanMail interface

You can choose to scan selected directories and subdirectories and/or selected databases from the ScanMail configuration screen.

Scanning selected directories from the Notes client

Directories can only be selected in the **Scan directories** section. Type the name of the directory to be scanned in the text box.

Note: You can select only one directory at a time to scan.

To scan the subdirectories also that are contained under the directory you specified, select the **Include subdirectories** check box. For example, you may select to scan all directories under your Notes drive. Enter `c:\lotus\domino\data` for the directory to scan on an R5 server, and check **Include subdirectories**.

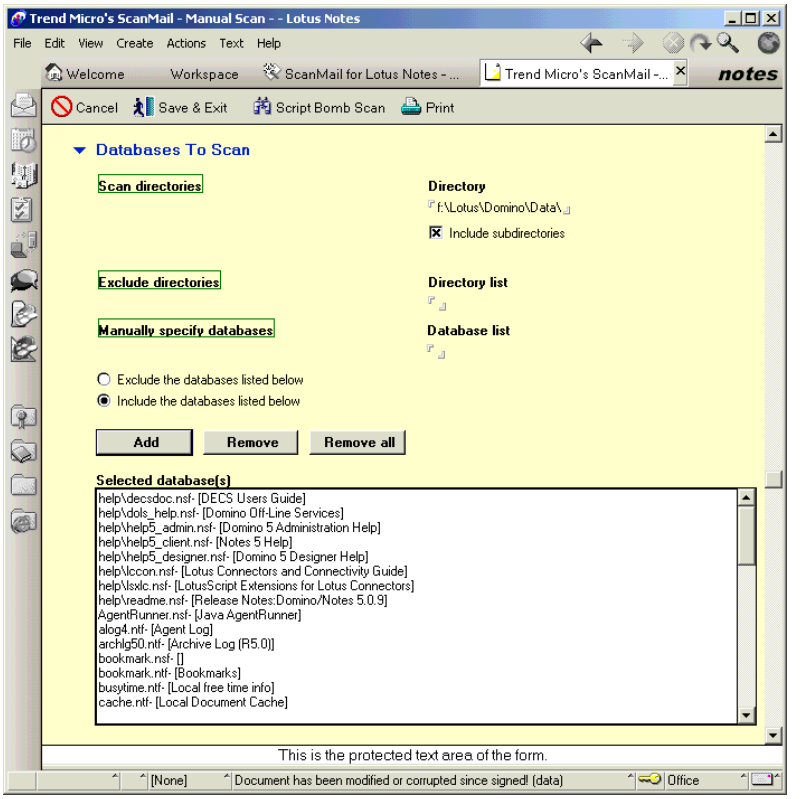


FIGURE 6-1. Manual Scan, Databases to Scan configuration section.

Note: Scanning directories and subdirectories allows a “wildcard” operation, equivalent to `*.nsf` and `*.ntf` for the path(s) specified.

To further specify which directories to scan, you can enter directories to omit from scanning in the **Exclude Directories** list. Enter the directories you want to exclude, separated by commas. This option overrides subdirectories selected in the "Include subdirectories" section above.

For example, if there are some directories in your data directory that you would like to exclude from scanning, you would enter them here:

```
c:lotus\domino\data\doc, c:\lotus\domino\data\help
```

You can configure specific databases that you do not wish to scan within the subdirectories by selecting the **Exclude the databases listed** below check box. Then select the **Add** button and check which databases you would like to exclude from scanning.

Scanning selected databases from the Notes client

To scan selected databases within directories, under the heading **Manually specify databases**, enter the path and name of the database you want scanned in the **Database list** field. Delimit multiple entries with a semicolon. This option is particularly useful when you’d like to scan databases that are stored outside the Notes directory. For example,

```
c:\test
```

-or-

You can also have ScanMail compile a list of databases in the Notes directory for you to select from.

Note: After making changes to the databases scanning options for Manual or Scheduled Scanning, you do not need to stop and restart the Notes server.

To select databases for scanning from the Notes client console:

1. Select **Include the databases listed below**.

2. Click **Add** and choose, from the list that appears, the databases you want scanned. Click a database to select it. You can select multiple databases simultaneously, then click **OK**. (Directories cannot be selected in this window).

   You'll notice that ScanMail runs a quick cleanup script called **Delete all db-documents** before adding the database. This script does not act upon your databases; instead it deletes a temporary list of documents that ScanMail itself created.

3. Click the **Remove** button to remove individual databases from the list that appears if you do not want them scanned or the **Remove All** button to remove all your database selections. Click **OK** to remove the database names from the list.

Alternatively, you can exclude databases from scanning:

1. Select **Exclude the databases listed below**.
2. Follow Steps 2 and 3 in the previous section. Any databases listed will not be scanned.

Configuring the Action on Viruses

When ScanMail detects a virus in an attached file contained in a document during a Manual or Scheduled Scan, it acts only upon the infected file. The document's original rich text format and any uninfected files that were also attached are not affected.

As for the infected file, specify one of four actions for ScanMail to take:

- **Pass** — to skip the infected file *without cleaning*. A warning message including the details specified in the Notification section is generated and sent to the designated Administrator.
- **Quarantine** — to remove the infected file from the document and move it, without cleaning, to the quarantine database. The quarantine database name is `smquar.nsf` in the `\data` directory on the Notes server where ScanMail is installed.
- **Delete** — to remove the infected file from the document and delete it from the server. The Notes administrator and any others designated are sent a notification message via email.
- **Auto Clean** — to have ScanMail automatically clean the infected file(s).

Action on uncleanable files

In some cases due to the nature of the virus, it can be identified but cannot be cleaned. When that happens, you can have ScanMail delete the infected file, move it to the quarantine database, or leave it in place without cleaning.

Configuring virus notification

When a virus is discovered during a database scan, ScanMail automatically alerts via email the people you designate—for example, the Notes administrator or other individuals who need to know when infected files are found.

Additional details about the virus are also included, such as the name of the infected database, the virus name, and the action ScanMail took. This information is also archived in ScanMail's log file. You can use ScanMail's default alert message, or compose one of your own.

To configure a virus notification:

1. Select the check box **Warning to administrator(s):**.
2. In the **Administrator(s)** field, type the email address of the person you want notified. ScanMail can send the alert to more than one person. Use a comma as the delimiter between addresses.

   Alternatively, you can click the drop-down arrow and select from the list of names that appears. Any address in the public & personal address books is eligible for this notification, including SMTP addresses.

   To compose the message you want the Administrator (and anyone else) to receive, type your message in the associated text field. For example,

   Administrator: ScanMail for Lotus Notes has detected a virus during a database scan.

Note: To use a multiple line notification message, press the "Enter" key between lines.

This message is automatically sent to the person(s) indicated whenever ScanMail detects a virus.

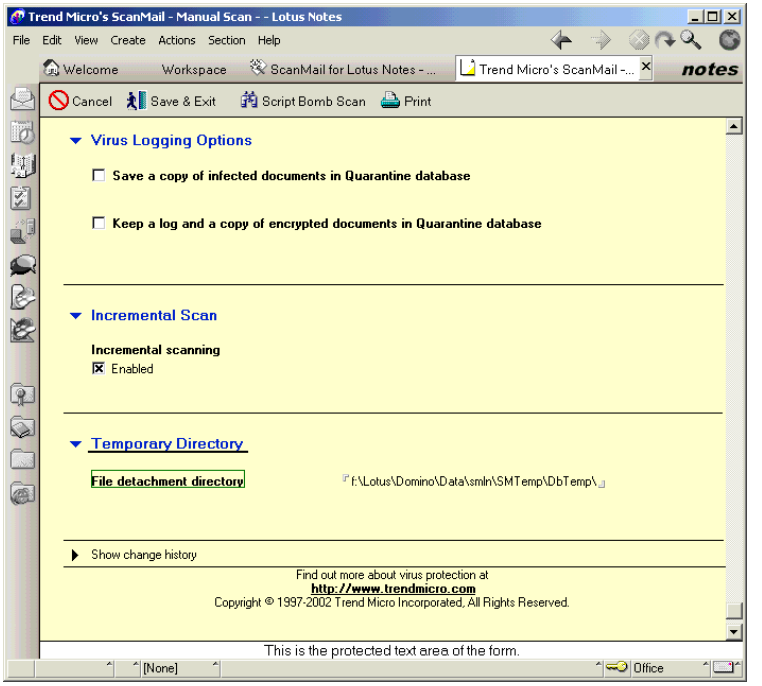


FIGURE 6-2. Manual Scan Configuration screen, bottom section with Warning to Administrators, Virus Logging, and Incremental Scanning enabled.

Virus logging options

The Virus Logging options are not selected by default. Select the check box(es) if you would like to enable these options.

- **Save a copy of infected documents in Quarantine database** — if you do not save a copy of infected documents, they will be deleted from your system. When you enable this option, a full copy of infected documents is saved in `\data\smquar.nsf`.

This option differs from the option to quarantine documents in that the quarantine database `\data\smquar.nsf` contains infected attachments only if they were uncleanable or if you selected not to clean them. The Quarantine database contains a copy of infected documents, whether or not the documents were subsequently cleaned and sent to the recipient.

- **Keep a log of encrypted documents in Quarantine database** — To keep a log of which documents were encrypted and thus could not be scanned on the server, select the second check box (encrypted files cannot be opened except by the original intended recipient).

Incremental scanning

Select the check box to enable **Incremental Scanning**. Incremental Scanning can save considerable server time and resources by allowing selective scanning of new and newly modified documents only.

Scanning is performed only on documents that have not been scanned or that have not been modified since the last scan. We recommend that you initialize the incremental scanning process by scanning all files on the server.

Specifying the temporary directory

Unless you specify otherwise, ScanMail will create and use the following temporary directories for Manual and Scheduled database scanning:

```
c:\SMTemp\DbTemp – for Manual Scans
c:\SMTemp\PTemp – for Scheduled Scans
```

If you would like to specify different temporary directories to use, you can change the default settings.

Script bomb scanning

ScanMail has the ability to scan Lotus Notes scripts for malicious code. Under **Database Scan**, select **Manual Scan** or **Scheduled Scan**, then select the **Scan for script bombs** check box in the "Scan Options" section. Select the **Script Bomb Scan** button at the top of the screen. By default, script scanning is not enabled.

Performing a manual database "Scan Now"

To perform an immediate scan from the Manual Scan Configuration screen:

1. Click **Scan Now** at the top of the screen to have ScanMail check the databases and directories you specified in the configuration screen.
2. Enter your local server (fully qualified) if prompted, for example:

   ```
   server1/OU1/US
   ```

3. In the **Server console** command field, enter the following command:

   ```
   load dbscan
   ```

4. Click **Live console** if you want the server output from the scanning session redirected to the current view screen.

   -or-

   Click **Send** to begin the scan. The databases and directories specified in the previous configuration screen are scanned. Depending on the size and number of databases, you may have to wait until the scanning process is finished.
5. Click **Done**.
6. To save your manual scan configuration settings, click **Save & Exit**.

Scheduling a database scan

Under **Database Scan** in the left navigator pane, select **Scheduled Scan**. The Scheduled Scan Configuration screen appears with the same options as are used in the Manual scan, with one new button at the top — **Schedule Scanning**

To schedule Database scans:

1. Select **Scheduled Scanning**, then click **Add Program** in the Action bar to render a screen for editing.
2. In the **Program name** field, enter the filename of the ScanMail database scanning program: **`pscan`**. Leave the next field, **Command line**, blank.

3. Choose the Notes server that has the databases you want scanned by clicking the drop-down arrow to the left of the **Server to run on** field and double-clicking the server name.
4. In the **Comments** field, you can enter a note of explanation about the scheduled program. For example,

   ScanMail for Lotus Notes Scheduled database scan.
5. You can set the status of the program to one of three states: **Enabled**, **Disabled**, or **Startup Only** (which launches Pscan whenever the Notes server is started).
6. Set the time, repeat interval, and days you want the database scanner to run. When you've finished, save and close the screen.

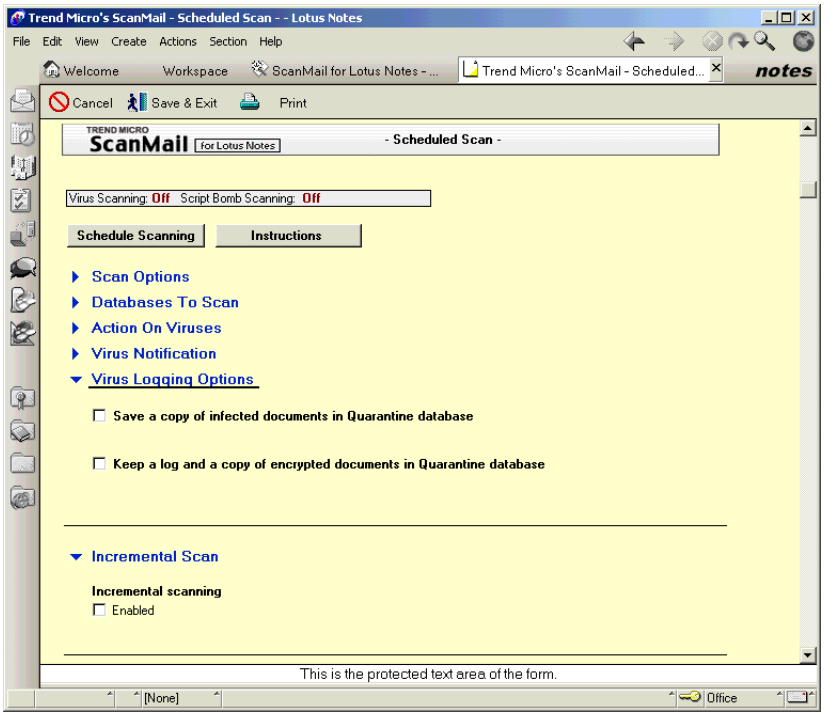


FIGURE 6-3. The configuration screen for Scheduled Scans.

Your scan will automatically run on the day and time you have selected each week.

Saving the new configuration

To save the new configuration, click **Save & Exit** (Notes client) or **Save** (Web browser), located at the top of the screen. To cancel your changes and revert to the last saved configuration, click **Cancel**.

Chapter 7

Using eManager

eManager is an optional ScanMail component that specializes in content filtering and spam control. It is automatically installed at the same time as ScanMail, but expires after 30 days if a serial number is not entered. There is no separate process for removing eManager.

Using eManager's content filtering, you can have eManager block, log, or postpone inbound and outbound email messages on the basis of:

- Message content (keyword or phrases)
- Attachment content (keyword or phrases)
- Attachment size, name, and/or type
- Mail size
- Sender's and/or Recipient's email address
- Message subject

Examples

- Control virus outbreaks immediately (such as the Melissa virus) by creating a filter rule to block all messages containing the subject "I love you".
- Stop spammers from annoying your mail users and wasting company time.

- Guard against harassing, illegal, and/or offensive content from being spread via your corporate mail servers.
- Manage bandwidth by postponing, until after normal business hours, the delivery of any messages To: or From: a particular domain, or sender.
- Block messages containing an attachment larger than a given size (but deliver smaller attachments in the same message as usual), or block the message if the total size exceeds a limit you set.

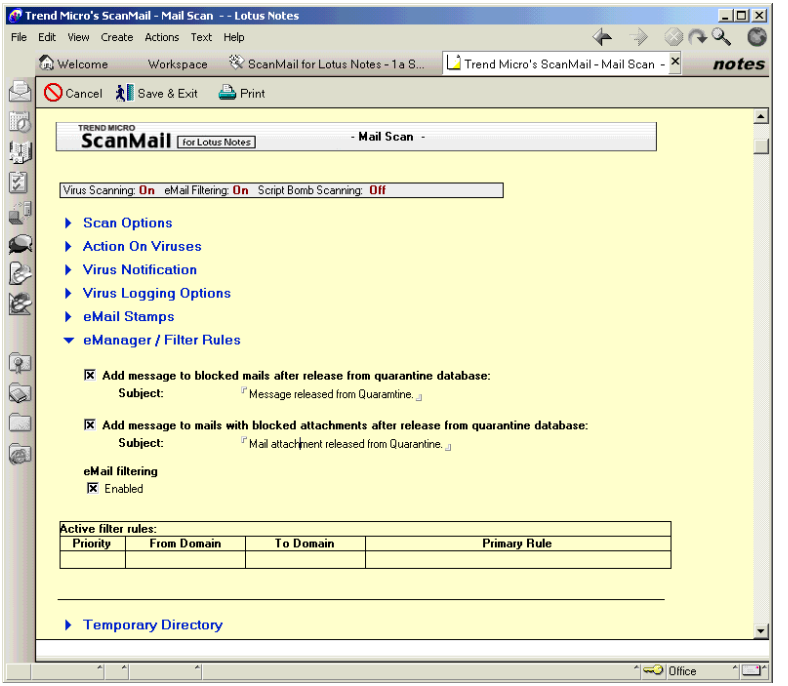


FIGURE 7-1. eManager, an optional ScanMail component, provides spam filtering and content management.

Sending your spam to Trend Micro

If you receive a spam message that eManager fails to detect, forward it (including all mail headers) to spam@trendmicro.com so it can be reviewed and added to the list.

Trend Micro employs a large team of spam collectors who work 24x7 to identify unique characteristics of spam email and add them to the list. Since spam senders frequently change their email addresses, characteristics such as web sites or telephone numbers are used to detect them. In addition, old, or "stale" data is removed from the list.

Updating the spam list for anti-spam filtering

Spam filtering works by comparing the header and body fields of inbound messages to a list of known as spam "signatures." These signatures include tell-tale signs such as a domain known to originate a lot of spam, habitual senders, and unique message content such as email addresses, URLs, and phone numbers. To stay current with the ever-changing spam list, you should schedule automatic list updates.

To schedule automatic list updates:

1. In the main ScanMail configuration menu, click **Update > Update Setting**.

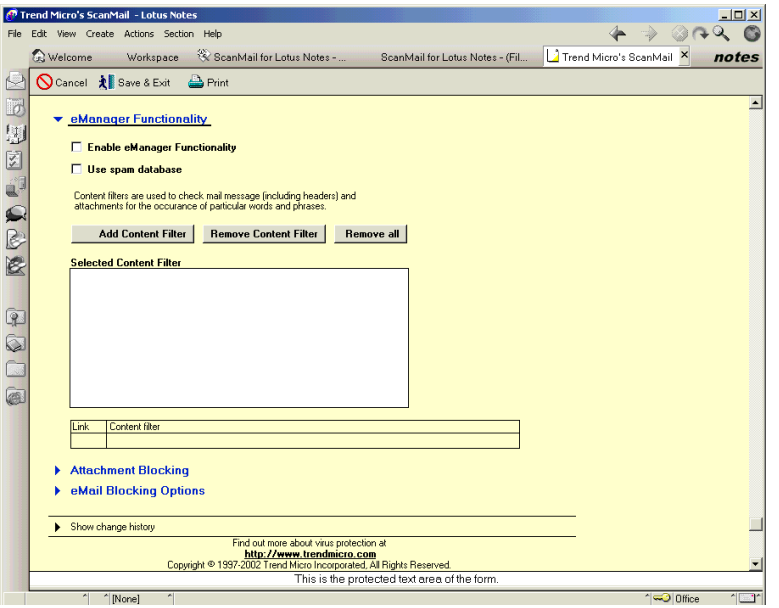


FIGURE 7-2. We recommend you automate virus pattern updates by scheduling the task to occur at least weekly.

2. Spam "match lists" are downloaded with the virus pattern file, so select at least **Virus pattern** and specify **Active Update server** for **Virus pattern files.**
3. If there is a proxy server between the ScanMail server and the Internet, identify it under **Proxy Server Settings**, by specifying the host name (or IP address) and port. Provide log on credentials for the proxy if required.
4. Click the **Load Pattern Update** button at the top of the screen, or go to the command line and enter,

   ```
   load pupdate
   ```

5. Click **Save and Exit**.

Blocking spam with eManager

ScanMail's eManager component allows you to block thousands of the known spam messages actively circulating the Internet from entering your network. Spam blocking occurs before the mail is processed by your Notes mail server. Blocked spam messages can be saved for individual review later, or deleted.

The spam filter detects spam messages in real-time, and before the message is delivered to the Notes mail server for distribution.

Matches are detected by comparing inbound message content with the list of thousands of spam signatures contained in Trend Micro's proprietary spam list. Updated lists are published daily, and can be downloaded automatically with the virus pattern file.

To block spam:

1. From the eManager configuration database, choose **Scan Options > Mail Scan > eManager / Filter Rules** and select **Filter Rules > All Filter Rules**. Click the **Create new rule** button that appears at the top of the page.
2. Select **Activate filter rule** to enable the rule.
3. Type a unique number in the **Priority number** field.
4. In the **From: Domain** field enter a * to check all inbound messages to see if they are spam.
5. Open **eManager Functionality**, and select both the **Enable eManager Functionality** and **Use spam database** options.
6. Click **Save & Close**.

Notes:

- Notifications for blocked spam are sent as usual, just like for other blocked mail.
- The Filter rule you create for spam blocking should not contain any other criteria (other than what is specified above).
- Spam matches are logged and can be viewed in the **Quarantine Manager**.
- Spam "match lists" are automatically downloaded with the virus pattern file if you use the ActiveUpdate option—it is recommended that you schedule this event to occur no less often than weekly.

Stopping a mass-mailing virus using eManager

Mass-mailing viruses (or "worms") emerged in the year 2000 and, within the space of a few hours, proved themselves to be particularly potent threat. Within a day, the Melissa (or ILOVEYOU virus had spread around the world, causing such a commotion that unprotected companies were forced to shut down their mail servers until the problem could be sorted out.

You can have eManager prevent such outbreaks from bringing down your network.

To block messages based on Subject or attachment name:

A. Create an Expression

1. In the eManager Configuration database, click **Scan Options > Mail Scan > eManager / Filter Rules**, and then choose **All Expressions > Create Expression**.
2. In the **Expression** field, enter a unique identifier, such as the Subject ("ILOVEYOU" during the Melissa outbreak), or a file attachment ("ANNAKOURNIKOVA.JPG.VBS" during the Anna Kournikova outbreak), and **Save & Exit** the screen.

Note: Check www.trendmicro.com during an outbreak for case-specific advice about creating a unique identifier.

B. Create a Content Filter to hold the Expression

1. From the main ScanMail menu, choose **All Content Filters > Create Content Filter** and select **Advanced Content** filter.
2. Begin filling out the **Content Filter** form by assigning a number and name to your form, for example "1", (if its your first rule) and "Melissa".
3. Choose **Mail header** and **Subject** to have eManager check these fields for your Expression (the unique identifier created in steps 1 and 2).
4. Choose **Mail body** to check the message content for a match.
5. Choose **Mail attachment** and **File name** to focus the search on attachments only (most efficient for Anna-Kournikova-type mass-mailing situations).
6. Next, click **Applied Expression** and the **Add Expression** button and then choose the Expression you just created from the list that appears and click Save & Exit.

C. Create a Filter Rule to govern the Content Filter

1. Once again at the main ScanMail menu, choose **All Filter Rules > Create new rule**.
2. Select **Activate filter rule** to enable the rule.
3. Type in a number such as "1" in the **Priority number** field.
4. In both the **From:** and **To:** domains, enter a ***** {wildcard} to have eManager check all messages. Otherwise, if you specify a particular domain, only messages **To:** or **From:** that domain are checked against the remaining criteria. See **Using Advanced Content filters** for important details about the **To:** and **From:** fields.
5. Open **eManager Functionality** and add the **Content Filter** you created in section **B**.
6. Click **Save & Exit,** and return to the main ScanMail menu.

D. Confirm that you have eMail Filtering enabled

1. At the main ScanMail menu, choose **Mail Scan**, scroll to the bottom of the page, and open the **eManager / Filter Rules** option.
2. Double-check to be sure **eMail Filtering** is **Enabled**, and confirm that your current **Filter Rule** is active and appears in the list of **Active Filter Rules**.
3. On the same page, after you choose your **Notification** options, click **Save & Exit** at the top of the page to apply the filter.

Using operators

eManager's mail filtering supports the following operators (listed in order of priority, operator name is followed by definition):

Note: Operators must be upper case. Operators must be offset by a . (period) on either side, buffered on either side by a space.

- **.(., .).—**grouping operator; used to change the evaluation order. The expression in these operators is evaluated first.
- **.WILD. * —**Wild card searches always start with **.**WILD**.** and a match will occur if the content contains the operand. For example, type in .WILD. *mobile to match on mobile, automobile, bookmobile, snowmobile, immobile. Or, type in .WILD. rain* to match on rainbow, raincoat, raindrop, rainy, rainstorm.
- **.OCCUR.—**allows you to filter by a keyword expression's prevalence (preset in eManager at 1). If the number of occurrences of the operand is greater than or equal to the preset number, this condition is triggered.
- **.NOT.—**must be used in conjunction with a second operator; NOT specifically excludes the word or phrase from the search.
- **.NEAR.—**filters by proximity (preset in eManager at 5). If the token count between the last token of the first operand and the last token of the second operand is less than the preset number, the condition is triggered.
- **.AND.—**links two or more keywords so the occurrence of both is required for criteria to be met.
- **.OR.—**links two or more keywords so the occurrence of *either* is required for criteria to be met.

Note: The operand and the operator must be separated by a space. An operand may also contain several tokens. A legal keyword expression is composed of tokens, which is the smallest unit used to match the expression to the content. A legal token can be an operator or the operand.

About Expressions

Although you can attach more than one Expression to an **Advanced Content Filter**, generally speaking it is best to keep filters as narrowly focused as possible. A given Content Filter should contain a *maximum* of one or two Expressions.

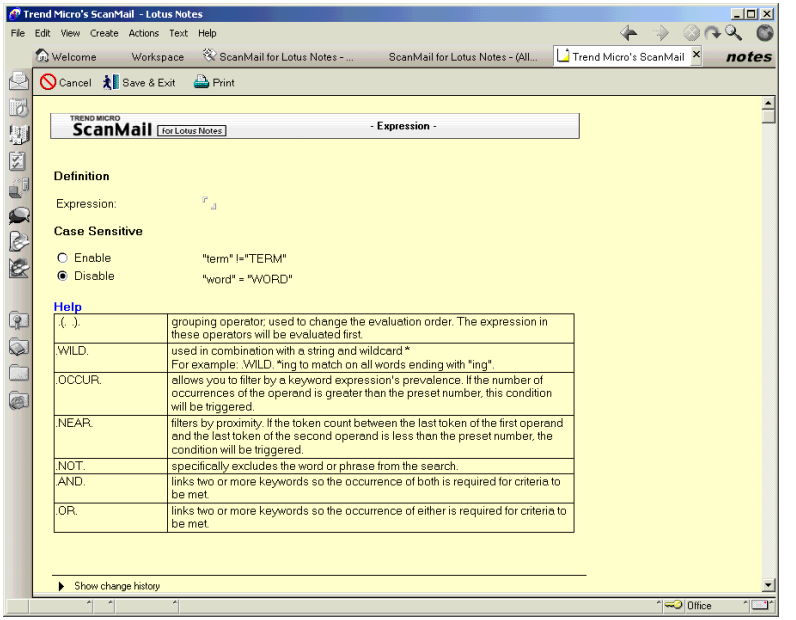


FIGURE 7-3. To specify a search criteria directly (without attaching an Expression) use a General Content Filter.

Notes

- Expressions contain the specified search parameters to be used by eManager.
- Use an Advanced Content Filter to specify in what portion of the message to search for the Expression.
- Use a Mail Filter Rule to define which messages to check for the Expression, and what action(s) to take whenever a match occurs.

Creating Expressions

Expressions are the root element of an Advanced Content Filter that allows you to define the key words or phrases that eManager should check for. You can create a new Expression for each word, phrase, or concept you want to filter, or include multiple search criteria into a single Expression.

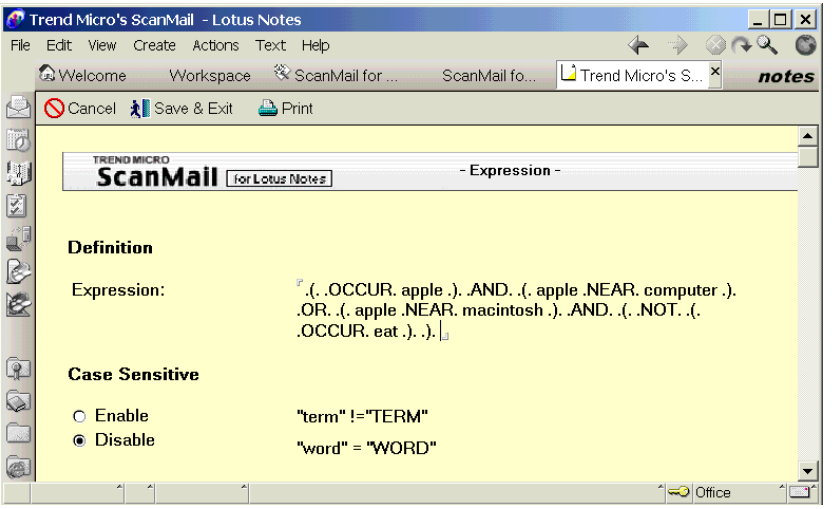
To create an Expression:

1. Click **Scan Options > eManager /Filter Rules > All Expressions**.
2. Click **Create Expression** in the button bar at the top of the screen.
3. In the **Expression** worksheet, enter the word or phrase you want to filter, and set the case properties you want to apply.

Note: Before enabling a new Expression, always test it first to be sure there are no unexpected consequences (and choose **Quarantine** rather than **Delete**).

Creating Compound Expressions

You can create a new Expression for each word, phrase, or concept you want to filter on. Or you can include multiple search criteria into a single Compound Expression.



To create a Compound Expression:

1. Click **Scan Options > Mail Scan > eManager > All Expressions**.
2. Click **Create Expression** at the top of the screen.
3. In the **Expression** worksheet, enter the first word or phrase you want to filter for connected by the logic of the operands.

Note: Be sure to leave a space before and after each operand in the expression. In addition, do not use line breaks or carriage returns within a single expression. It is better to create two expressions, instead.

For example, to create a (very complex) rule to distinguish between "apple" fruit and "apple" computer, you may want to construct a rule such as the following:

```
.(. .OCCUR. apple .). .AND. .(. apple .NEAR. computer .). .OR. .(.
apple .NEAR. macintosh .). .AND. .(. .NOT. .(. .OCCUR. eat .). .).
```

This rule triggers a match if the word **Apple** occurs two or more times in a document, and within 25 words either way of the word **computer**, or if the word **Macintosh** occurs in the document, this also triggers a match. But if the word **eat** also occurs in the document—a match is not triggered.

However, we recommend that you keep your expressions simple and narrowly defined. So, instead of one very complex rule as shown above, we recommend that you create two simpler rules and attach each to a Mail Filter Rule.

Expression 1.

```
.(. .OCCUR. apple .). .AND. .(. apple .NEAR. computer .).
```

Expression 2.

```
.(. apple .NEAR. macintosh .). .AND. .(. .NOT. .(. .OCCUR. eat .).
.).
```

Note: When multiple Expressions are attached to a single Mail Filter Rule, the OR operator is used to between them.

Using wildcards in an Expression

Only Expressions support the use of wildcards—the General Content filter does not.

To use wildcards in an Expression:

1. Click **Scan Options >eManager > Filter Rules > All Expressions**.
2. Next, click **Create Expression** in the button bar at the top of the screen.
3. In the **Expression** worksheet, enter the word or phrase you want to find using `.WILD. *`*expression* or `.WILD. express*`

Examples

`.WILD. This * message`

This expression matches content when the word "message" follows the word "This". There can be any number of words between the word "This" and the word "message".

Content Result

- Match: ...**This message** is being sent to you because you signed up for our free email newsletter...
- Match: ...**This** is to inform you that I will be on holidays until 10/12. You can leave a **message** at 408-555-1212...
- No match: ...**This** is arguably the most exciting software that I have...
- **.WILD. *ing**

This expression matches any content which ends with "ing".

Content Result

- Match: ...that movie has a surprise end**ing**...
- Match: ...this should be the beginn**ing** of a mutually productive...
- No match: ...The iron **ing**ots were loaded on to the freighter...

Note: Before enabling a new Expression in a Mail Filter rule, always test it first (and choose to **Quarantine** rather than **Delete**) to prevent any undesired or unexpected consequences.

Advanced and General Content Filters

The Content Filter includes two form options: **Advanced**, and **General**.

Use the **Advanced** Content Filter if you want to:

- Create a complex filter, including one or more Expressions
- Create a filter using multiple Expressions, linked via the "or" operator
- Scan the message body only
- Scan attachment content only
- Focus your search on a particular message header field such as: **Subject, To: cc: From:**
- Set up a match threshold for the occurrence of a particular attachment (for example, don't block a message unless a certain number of matches of the specified attachment have occurred—useful, for example, for mass mailing viruses which tend to propagate widely and may include attachments of a common name).
- Include additional values for .OCCUR.
- Include additional values for .NEAR.

Use the **General** Content Filter to:

- Quickly create a rule (without first creating an Expression)
- Filter messages based on the text appearing in the Subject
- Filter messages based on the text appearing in the Body (all or some keywords)
- Filter messages based on file attachment name

Using General Content Filters

A General Content Filter can be used, for example, to specify what to search for (such as keyword or phrase) and where to search for it (in the Subject, body, attachment, etc.) all from a single page.

After creating a **General Content Filter,** be sure to create a **Mail Filter Rule** to specify which messages to search and also what action to perform upon finding a match. You can use the following information to help correctly fill out a General Content Filter worksheet:

- **Content filter number**: A user-assigned number to help identify the rule when it appears in a list of rules. Use whole numbers only, zero is not valid.

> *Tip:* Rather than number each new rule 1, 2, 3, 4, as you create it, number rules by 10's—10, 20, 30, 40. This allows you to later "back-fill" new rules as you develop themes.

- **Content filter name:** A user assigned name to help identify the rule when it appears in a list of rules. Although there is no limit to length, a succinct name may be more useful when it appears in the narrow column of the rule list.
- **Subject line**: Type the text of the Subject here. Typically, the Subject is known and specific—for example, ILOVEYOU, for the Melissa mass-mailer virus—and may even be copied directly from the problem message and pasted directly into the filter. Wild cards are supported in this field.
- **Mail body contains**: Type the keyword or phrase you want to search for here. Wild cards are supported here.
- **Attachment file name contains**: Type the file name you want to search for here. Wild cards are supported.

> *Tip:* Although you can add Mail Filter rules to your Content Filter, it is generally better to add Content Filter rules to a Mail Filter.

Using Advanced Content Filters

Use the following information to help correctly fill out an Advanced Content Filter worksheet:

- **Content filter number**: A user-assigned number to help identify the rule when it appears in a list of rules. Use whole numbers only, zero is not valid.

> *Tip:* Rather than number each new rule 1, 2, 3, 4, as you create it, number rules by 10's—10, 20, 30, 40. This will allow you to later "back-fill" new rules as you develop themes.

- **Content filter name:** A user assigned name to help identify the rule when it appears in a list of rules.

- **Mail header**: Select the **Mail header** option by itself to include all header fields in the search. Alternatively, you can specify one or more individual fields, including **Subject**, **To**: **From**: and **cc:**.
  - When using ScanMail eManager to create filter rules, (from the main ScanMail menu, click "Scan Options > eManager / Filter Rules") you must specify a value for either the "From:" field, the "To:" field, or both.
  - If a value is specified in both the To: and From: fields, the OR operator is used (the occurrence of any one of the values will trigger a match).
  - Values can be a wildcard (*)to apply the rule to all mails, a domain (*@spamnet.com), or an individual (tom@spamnet.com).
  - See **Priority numbers and Address Filters** for more information.

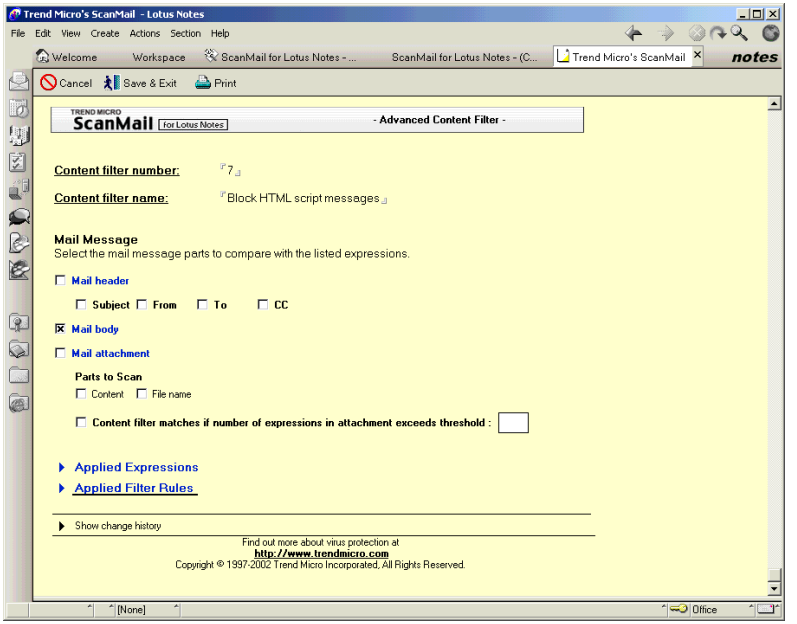


FIGURE 7-4. Use a short name when naming the content filter and it will be easier to read when it appears in the narrow rule-lies column.

- **Mail body:** Select this option to have eManager check the content of the message body.
- **Mail attachment > Parts to Scan.**
  - **Content**: Check this option to scan the entire content of the attachment for occurrence of the Expression.

> **Note:** **Note**: Checking the **Content** option may slow overall mail processing performance.

  - **File name**: Check this option to check only the file name for occurrence of the Expression.
  - **Content filter matches if number...** The number entered here is completely dependant on what type of filter it is being applied to. For example, a single instance of a racial slur may be sufficient grounds to trigger the filter. On the other hand, if you are filtering for a potentially ambiguous word such as "resume" (which could be either the verb, "to start again," or the noun for "a list of professional accomplishments") you may want to filter for two or more occurrences to increase the likelihood of it being the latter.

Creating a Content Filter

Content Filters define where in the message to look for the keywords or phrases.

To create a Content Filter:

1. Click **Scan Options > Mail Scan > eManager > Content Filter**.
2. Click **Create Content Filter** at the top of the screen. The following choices appear:
   - **Advanced Content Filter.** Choose this option if you want to include one or more Expressions, or if you want to be able to "aim" the filter at the message header, body, and/or attachment. The Advanced filter allows you to use, as a part of the rule definition, one or more Expressions, and one or more Mail Filter rules.
   - **General Content Filter**. Choose this option if all you want to do is create a rule "on the fly" — a word or two to check for in the Subject, body, or attachment content.

3. Fill out the work sheet as appropriate.

Note: You can create a series of "base" content filters that define what portions of the message to scan, and use these again and again as elements of your Filter rules. For example, create one Advanced Content filter for scanning Subject, another for Attachments, and another to include all parts of the mail and then use these as building blocks for your Mail Filters.

Blocking messages on the basis of content

eManager can check the body and attachments of email messages for the occurrence of a given word, words, or phrase. For example, a Filter Rule could be created to enforce a corporate policy against the use of certain objectionable words, another one for discriminatory words, and another for potentially libelous content,

To block messages based on content:

A. Create one or more Expressions

1. In the eManager Configuration database, click **Scan Options > Mail Scan > eManager / Filter Rules**, and then choose **All Expressions > Create Expression** from the button bar.
2. In the **Expression** field, enter the keyword or phrase you want to "search" the messages for—for example, the word "Resume", and then **Save & Exit** the screen.
3. Create one Expression for every word or phrase you want to include. To distinguish "resume" (to start again), from "resume" (curriculum vitae), you might want to create one or more additional Expressions such as: "career", "interview", and "job".

Note: Multiple Expressions attached to the Advanced Content form are linked via Or operator—the more Expressions included, the greater the probability of a match (and greater likelihood of false positives), whereas multiple keywords specified in the General Content are linked via And operator—the more keywords specified, the lower the probability of a match.

B. Create a Content Filter to hold the Expression

1. From the main ScanMail menu, choose **All Content Filter > Create Content Filter** and select **Advanced Content** filter.
2. Begin filling out the **Content Filter** by assigning a number and name to the form. Choose a short name that indicates the purpose of the rule, for example, Resume.
3. Complete the form by specifying notification options, etc. Click **Applied Expression** and **Add Expression**. Choose the Expression(s) you just created from the list that appears.
4. Click **Save & Exit.**

C. Create a Filter Rule to govern the Content Filter

1. On the main ScanMail menu, choose **All Filter Rules > Create new rule**.
   - Select **Activate filter rule** to enable the rule.
   - Type in a number such as "1" in the **Priority number** field.
2. In the **From:** Domain field, enter a ***** (wildcard) to have eManager scan all inbound messages for occurrence of the keyword or Expression. See **Using Advanced Content filters** for important details about the **To:** and **From:** fields.
3. Open **eManager Functionality** and add the **Content Filter** you created in section **B**.
4. Click **Enable eManager Functionality**, then **Save & Exit,** and then return to the main ScanMail menu.

D. Confirm that you have eMail Filtering enabled

1. On the main ScanMail menu, choose **Mail Scan**, scroll to the bottom of the page, and open the **eManager / Filter Rules** option.
2. Double-check to be sure **eMail Filtering** is **Enabled**, and confirm that your current Filter Rule appears in the list of Active Filter Rules.
3. On the same page, after customizing the notification options, etc. click **Save & Exit** to apply the filter.

About Filter rules

Below are some example tasks you could use ScanMail's eManager and filter rules to achieve:

Virus security

- Prevent an active virus outbreak by creating a rule to stop all messages with a given Subject heading (for example, "ILOVEYOU")
- Prevent certain file types from entering the network via email attachment
- Block mail based on attachment name (often a key differentiation in mass-mailer programs)

Content security and policy enforcement

- Block all mail sent to or from a particular country or business
- Block messages containing offensive, or legally liable, words or phrases—including those found in attached documents
- Block resumes from being sent out by employees

Spam prevention

- Prevent spam from arriving with inbound mail
- Block all inbound mail sent from a particular domain (e.g., spam&garbage.com)

Bandwidth management

- Block messages with attachments larger than a given size; automatically notify sender of the mail policy
- Postpone the delivery of mail sent to certain time-zones until after peak local hours (but before start of the remote site's day)

Priority numbers and Address filters

Use the following information to correctly enter information into the Mail Filter Rule worksheet:

- **Priority number**: This number determines the order in which filter rules are processed, with the lower numbers coming before higher ones.

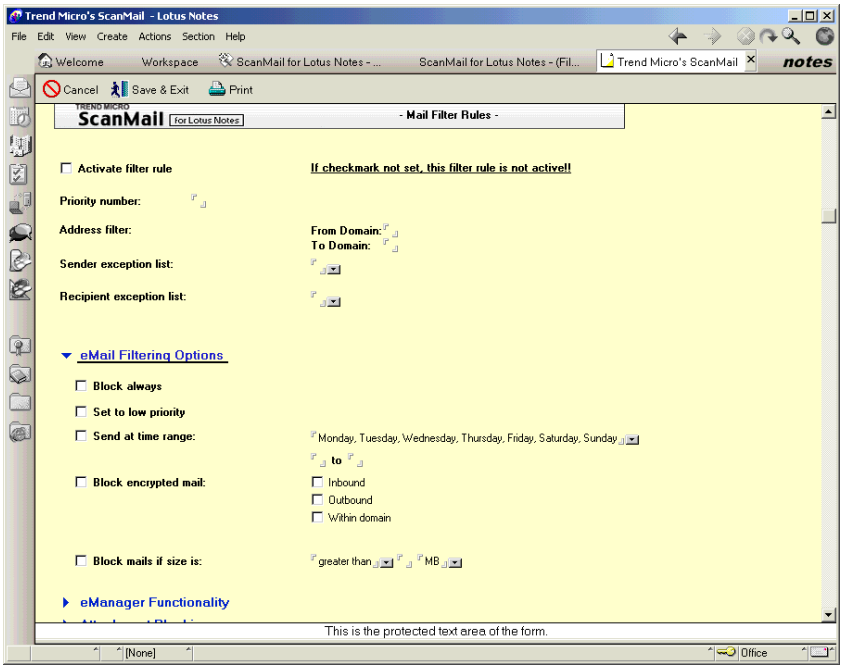


FIGURE 7-5. Rather than number each new rule 1, 2, 3, as you create it, number rules by 10's—10, 20, 30 so you can later "back-fill" new rules with higher priorities.

Tip: eManager proceeds downward through the list of rules based on the priority number, and stops processing rules as soon as a match occurs. As such, it can be more efficient to give the broadest rules — those with the greatest likelihood of producing a match—the highest priorities.

- **Address filter:** Specifies which messages the Filter Rule is applicable to. Examples,
  - To have the filter rule apply to *all inbound and outbound* messages, enter a wildcard `*` in either the **To Domain** or the **From Domain** field .
  - To limit messages being sent out of the organization, enter `*your-domain*` in the **From Domain** field (used, for example, as a part of a filter to check for offensive content in customer communications).
  - To scan only messages being sent internally, enter

    ```
    *your-domain*
    ```

    in the **To Domain** field (used, for example, as a part of a filter to block messages > 2MB from being sent via email).
  - To block all messages from a given sender or domain from being delivered to members of your organization, enter

    ```
    *domain*
    ```

    in the **From Domain** field (used, for example, to block spam from being sent from a particular domain).
- **Sender exception list:** Used in conjunction with the **To** and **From Domain** fields, the **Sender exception list** allows you to exempt certain users from the rule. Populate the field either by selecting names from the Notes Domino Directory or type individual internet email addresses (delimit multiple addresses with a comma).
- **Recipient exception list:** same as above.

Email filtering options

The email filtering options described below are optional *actions* you can have eManager take whenever a match is triggered between an active Expression or Content Filter and the criteria you defined in the **Address** filter.

Note: Additional **Email Blocking Options** that affect how the blocking you specify is carried out can be found at the bottom of the **Mail Filter Rules** page, including

notification options, quarantine options, and whether eManager should block the message, the attachment, or both.

- **Block always:** Select this option to immediately block the message, the attachment, or both whenever the sender or recipient matches what is specified in the address filter.
- **Set to low priority**: Select this option to have eManager mark as "low priority" all messages where the sender or recipient matches what is specified in the address filter.

Note: "Low priority" is a Domino routing setting, which, by default, means such mail will be held until between midnight and 6:00 a.m.

- **Sent at time range**: eManager can postpone delivery of mail that matches the Filter Rule by holding it in the `smtime.nsf` database. Select this option and

specify a day and time to until which eManager should retain matching messages.

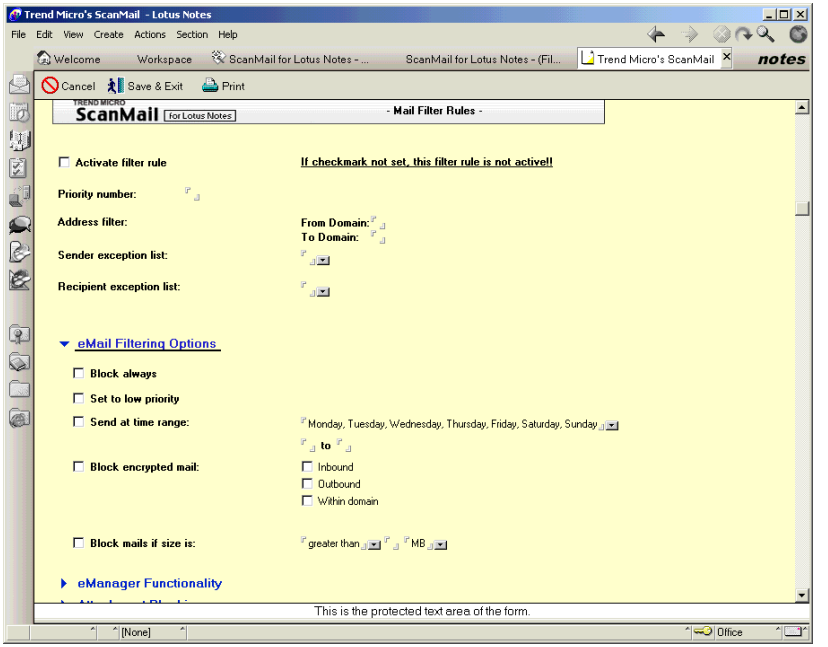


FIGURE 7-6. Scroll to the bottom of the page for additional options such as Save/Delete, notifications, and specifying whether to act on the entire message or attachment only.

- **Block encrypted mail**: Select this option to have eManager block encrypted mail as that also meets the criteria specified for the **Address Filter** (encrypted messages and their attachments cannot be scanned for content or viruses).

Note: **Note:** The **Block encrypted mail** action criteria is usually *not* used in conjunction with an **Expression** or **Content Filter)**,

---

- **Block mail if size is**: Select this option to have eManager block messages whose total size (including body and all attachments) meets or exceeds the size criteria

you have specified. **Note:** this action is usually *not* used in conjunction with an **Expression** or **Content Filter)**.

eManager Functionality

Features of the eManager Functionality option are explained below:

- **Enable eManager Functionality**—Choose this option to have eManager apply the conditions you defined in the Mail Filter Rule page to scanning the content of mail messages.
- **Use Spam Database—**Typically, you need only to enable this feature once—in one Mail Filter Rule—and that rule automatically covers all spam filtering. This default spam filter automatically draws upon Trend Micro's database of thousands of known spam senders, message subjects, and domains.
- **Add | Remove Content Filters**—After defining the criteria of what messages to scan and what action to perform whenever a message is triggered, add one or more **Content Filters** containing the **Expressions** or terms that you want to scan for.

Note: Although there are many exceptions, we recommend that you attach only one or two **Content Filters** to a given **Mail Filter Rule**. Adding too many Content Filters can have the result of either triggering too many matches, or, at the other extreme, too few.

Attachment blocking

Attachment blocking is used for blocking all or specified attachment types or names from being delivered to your system. This can be particularly useful in a virus outbreak. Specified attachments are blocked and therefore do not need to be scanned.

The following example illustrates how to set up a filter rule from the Notes client console.

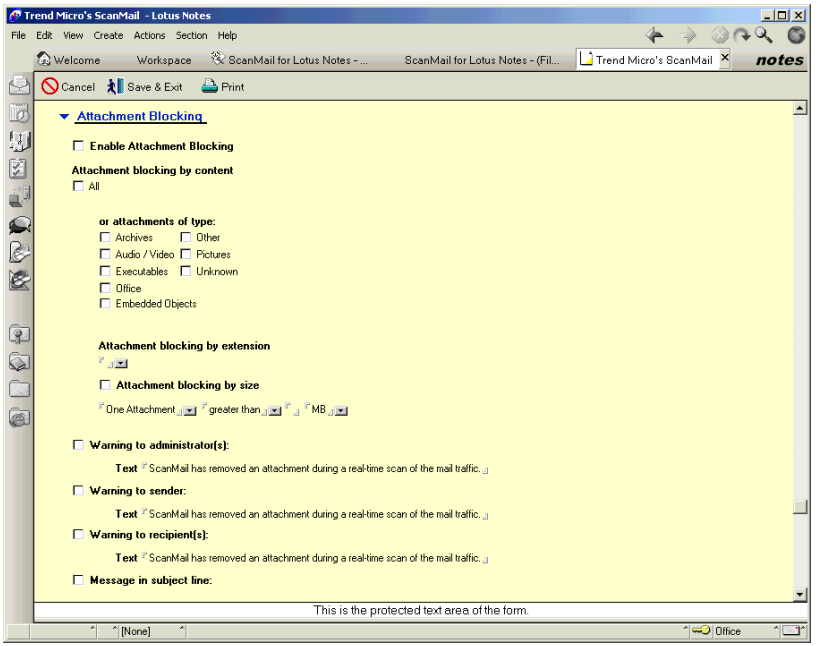


FIGURE 7-7. Mail Scan, Attachment Blocking section, Notes client console with Office and Executable attachments blocked except for user John Smith.

For the following example, selections are available for the Attachment Blocking by content section:

- Select **All** to block all attachment types. This is the most exclusive configuration; every email attachment is blocked, regardless of its extension.
- Alternatively, with the **Attachments of type** section you can select only certain types of attachments such as executables to block. All other attachments will be sent normally and submitted for virus scanning. Attachment blocking by type checks the true file type rather than just the extension name. Therefore, even if a Word document has the extension renamed to `.bak`, it will still be blocked.

- A less secure option is to do **Attachment blocking by extension**, wherein files are blocked by the exact extension name only, rather than by the type. Type in the extensions you want blocked from delivery, separated by commas or semicolons, for example, `*.doc; *.dot`. All attachments that match your specifications are blocked.

Note: In this case, only attachments with these exact extension names will be blocked. If a Word document is saved with the extension `.rtf`, for example, it will not be blocked. In addition, if a Word document was saved with the extension `.doc`, but renamed to `.bak`, it will not be blocked. To block all Office documents, select **Office** under **Attachments of type**.

A warning message can be sent to the administrator(s), sender, or recipient(s) when a file is blocked by selecting the respective check boxes. You can use the default message, or edit it to create a customized message. In the case of the administrator and sender, the alert is sent as a separate email, whereas for the recipient, it can either be appended to the original email that contained the infected file attachment, or included in a separate email.

Alternatively, the administrator can choose not to configure any type of notification to the recipient. To include a warning message in the subject line only, select the check box and then type the text to append to the subject in the associated text box.

Blocking messages on the basis of size

Corporate mail policies may limit the size of mail employees can send or receive. Limiting message size can be especially relevant when combined with virus and content scanning because scanning large attachments, especially compressed file attachments, can consume considerable CPU and memory resources.

To remove large attachments from email messages and notify the user of the action:

1. From the eManager configuration database, click **Scan Options > Mail Scan> eManager / Filter Rules**. Select **Filter Rules > All Filter Rules,** and click the **Create new rule** button that appears at the top of the page.
   - Select **Activate filter rule** to enable the rule.
   - Type a unique number in the **Priority number** field.

- In the **To Domain** field enter an * to include all recipients under the umbrella of this rule.

2. Click **Attachment Blocking** to open this option, then **Enable Attachment Blocking**, and **Attachment blocking by size**.
3. Specify whether you want to block on the basis of a single attachment or all attachments, and then enter the maximum attachment size. For example, **One Attachment | Greater than | 2MB** stops any message with a single attachment larger than 2MB, but not a document with ten 1MB attachments.
4. Fill out the attachment blocking notifications as needed, and click **Save & Close**. To remind users of an attachment-size policy, you can include text such as the following in the **Notification to Sender** field:

```
Dear email user: Files larger than 2MB cannot be sent
via email. Please use the FTP server to distribute large
files.
```

Note: To block mail on the basis of overall message size rather than size of attachment, open **eMail Filtering Options**, click **Block mail if size is:** , and specify a message size. This option differs from attachment blocking in that it includes objects pasted directly into the body of the email—a 50-page document could be attached, or the contents pasted into the email body, for example.

Email Blocking Options

eMail Blocking Options are an important part of **Mail Filter Rules**, especially as they govern the conduct of your rule.

- **Notification options—**whenever eManager finds a match, and the action specified in **Email filtering options** or **Email Blocking Options** is a blocking action, you can have eManager automatically send out notifications to the Notes administrator, the message sender, and/or recipient.
- **Save a copy of blocked mails...—**We recommend that you have eManager save a copy of all blocked messages in the Quarantine database, at least for the first week or two of applying a new **Mail Filter Rule**.
- **Block Mail** or **Block Attachment**—Whenever a content match is triggered for content that appears in a message attachment (rather than the message body), eManager can block either the entire message or the only the attachment.

Special case notes for content matches:

- If the message contains multiple attachments but only one triggers a content match, and the blocking option is set to block attachments, only the attachment with the content match will be blocked.
- If the message contains multiple attachments but only one triggers a content match, and the blocking option is set to block the entire message, the message together with the attachment is blocked.
- If the mail is addressed to multiple recipients and meets the two conditions specified below, the attachment will be blocked for *all* users, even if the recipients appear in the **Sender** or **Recipient exception** list:
  - **a.** An attachment blocked (in other words, a filter rule is triggered)
  - **b.** At least one recipient and/or sender does not appear on the exception list
- If the mail is addressed to multiple recipients, and the sender and all recipients appear in the **Sender** or **Recipient exception** list, the message will be delivered to all regardless of match.

Blocking, postponing, and/or monitoring messages

Content security can take many forms, including checking for leaked corporate secrets, offensive or inappropriate language, or even questionable contact with competitor corporations or hostile countries.

Bandwidth management, or the efficient allocation of finite corporate resources, can also take many forms and may include postponing all messages routed to a given time-zone until after peak local working hours, but before business hours at the remote site. Or, you may want local deliveries to satellite sites to take advantage of reduced telecommunication rates during midnight hours.

Note: eManager will delete blocked messages by default, unless you specify otherwise.

To block or postpone email messages on the basis of destination:

1. From the eManager configuration database, **Scan Options > Mail Scan > eManager / Filter Rules** and then select **Filter Rules > All Filter Rules** and click the **Create new rule** button that appears at the top of the page.
   - Select **Activate filter rule** to enable the rule
   - Type a unique number in the **Priority number** field
2. In the **To Domain** field enter the criteria you want to filter on, for example, a country, company, or Internet domain that you want to prevent (or monitor) contact with.
3. Select the **eMail Filtering Options** you want eManager to perform when a match occurs:
   - **Block always:** Select this option to automatically block either the message, the attachment, **To:** or **From:** the domain specified above, or whenever a match is found.
   - **Set to low priority**: Select this option to have eManager mark as "low priority" messages that trigger a match. **Note:** "Low priority" is a Domino routing setting, which, by default, means such mail will be held until between midnight and 6:00 a.m.
   - **Send at time range**: eManager can postpone delivery of mail that matches the Filter Rule by holding it in the `Lotus\Domino\Data\smtime.nsf` database . Select this option and specify a day and time to until which eManager should retain matching messages.
4. At the bottom of the screen, open **Email Blocking Options** and fill out whatever automatic notifications and blocking action that you want to occur whenever the rule is executed.
5. Finally, click **Save a copy of the blocked mail messages in the Quarantine database** if you do not want them to be deleted.

Note: Whenever using a new rule, it is always advisable to save a copy of blocked mail to the Quarantine database rather than delete them. Once you are sure your rule is free of unintended consequences, you can return and change the status off this option.

Preventing encrypted messages from entering the network

ScanMail does not scan files that have been encrypted, which means it is theoretically possible for viruses to enter a protected Notes Domino network via encrypted mail.

To prevent this, you can have eManager block the delivery of all encrypted messages. Blocked messages can be immediately deleted or saved to the Quarantine database, where they can be re-sent or deleted.

To block delivery of encrypted mail:

1. From the eManager configuration database, **Scan Options > eManager / Filter Rules** and then select **Filter Rules > All Filter Rules** and click the **Create new rule** button that appears at the top of the page.
   - Select **Activate filter rule** to enable the rule.
   - Type a unique number in the **Priority number** field.
   - In both the **From:** and **To:** domains, enter a ***** {wildcard} to have ScanMail check all messages. Otherwise, if you specify a particular domain, only messages **To:** or **From:** that domain will be checked against the remaining criteria.
2. Open **eMail filtering Options** and click **Block encrypted mail.** Choose Inbound, Outbound, Within Domain, or all three to block all encrypted mail.
3. Open **eMail Blocking Options** at the bottom of the page, and choose the notifications options you want.
4. Click **Save & Exit.**

Chapter 8

Log Maintenance and Statistics

ScanMail for Lotus Notes keeps a running log of all its activities. New logs are created whenever a virus is found and represent a valuable source of system information. The virus logs can be grouped by date, user, virus name, action, and service (real-time email scan, static database—manual and scheduled scan, or real-time database scan). Within each category, they are grouped under date (all dates, today, one week, and one month).

Individual virus log records contain a unique ID number for the document. They contain information on the server and database the document was found on, the attachment name and action on viruses found (or files blocked, or script bombs found). For greater security, a quarantine database is used to store infected documents that have been quarantined, rather than a quarantine directory. The quarantine logs are grouped by date.

ScanMail provides a Log Maintenance screen where you can determine how long to keep the log files and schedule regular log maintenance. Alternatively, you can manually delete the virus and quarantine logs. In addition, you can set up a log replication connection to replicate your virus logs to one central server.

In this chapter, we present several ways to view statistics and create reports. As in earlier versions of ScanMail, you can produce Virus Statistics reports from your virus logs over a given time period. The reports include the aggregate number of viruses by disposition—cleaned, deleted, quarantined, and passed. In addition, the total number

of files not scanned due to encryption, number of attachments blocked, and number and disposition of "Script Bombs" found is available.

This chapter covers viewing and deleting ScanMail's virus logs and quarantine logs, and generating virus statistics. The following topics are covered:

- Viewing the Virus Logs by date, user, virus name, action, and type of scan performed
- Viewing individual log details and the original documents contained in the Virus Logs
- Viewing the Quarantine Area
- Enabling and disabling deletion of individual log files
- Configuring Scheduled log deletion and deleting the original document copies
- Manually deleting logs and the original document copies
- Setting up Log Replication connections
- Generating virus statistics

About the log configuration screens

ScanMail for Lotus Notes has several configuration screens for the Virus and Quarantine Logs:

1. **Virus Logs** —query and analyze logs by date, virus, or scanner.
2. **Statistics**—provides top ten lists showing most common viruses, users with most virus incidents, most infected databases, etc. and provides graphical analysis of virus activity for a given server or group of servers.
3. Log Maintenance
   a. **Scheduled Log Deletion** — used to set up regular log maintenance to delete logs no longer needed on the server.
   b. **Manual Log Deletion** — used to delete individual or all logs immediately.
   c. **Log Replication** — used to create replications of the Quarantine database, for example, to a central server.

Viewing virus logs

ScanMail write its logs to the `smquar.nsf` database in the Notes data directory, typically, `\lotus\domino\data`.

To view the virus logs:

- From the main ScanMail menu, click **Logs > View Logs** and then choose the criteria by which you want to see the logs.

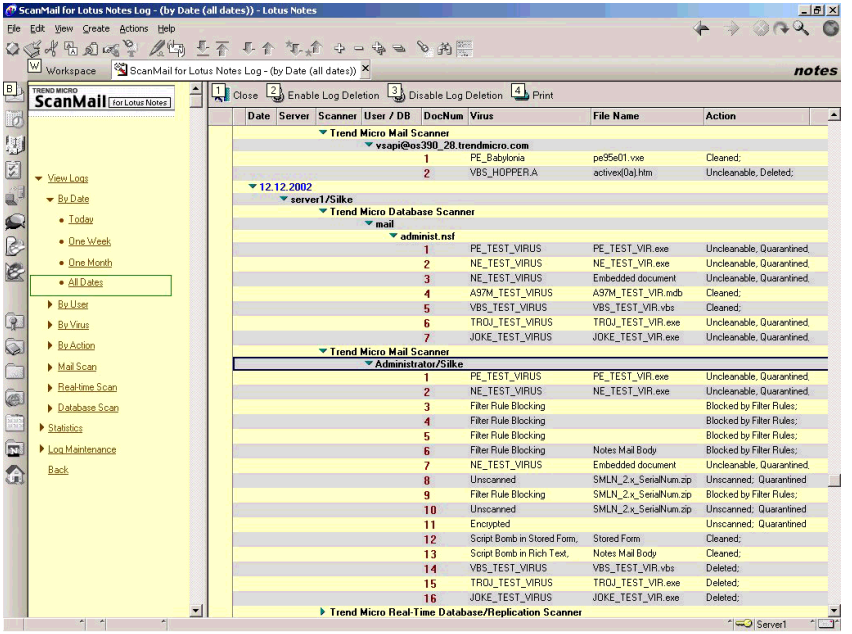


FIGURE 8-1. A view of ScanMail's virus logs by date showing viruses detected, files blocked, and encrypted documents that were not scanned.

Viewing virus log details

Each log, regardless of its group or time period, contains all the relevant details of the virus detection: the time and date it was discovered, the **Virus Name**, the **Attachment** it was infecting, the **Action** ScanMail performed (clean, pass,

quarantine, block, or delete), the **method of detection**, and, in the case of email, the email address of both the **sender** and **recipient**.

To view virus log details:

1. To display the log details, navigate by clicking the arrows until the list of virus logs itself appears.
2. Double-click one of the individual virus logs to display the details.

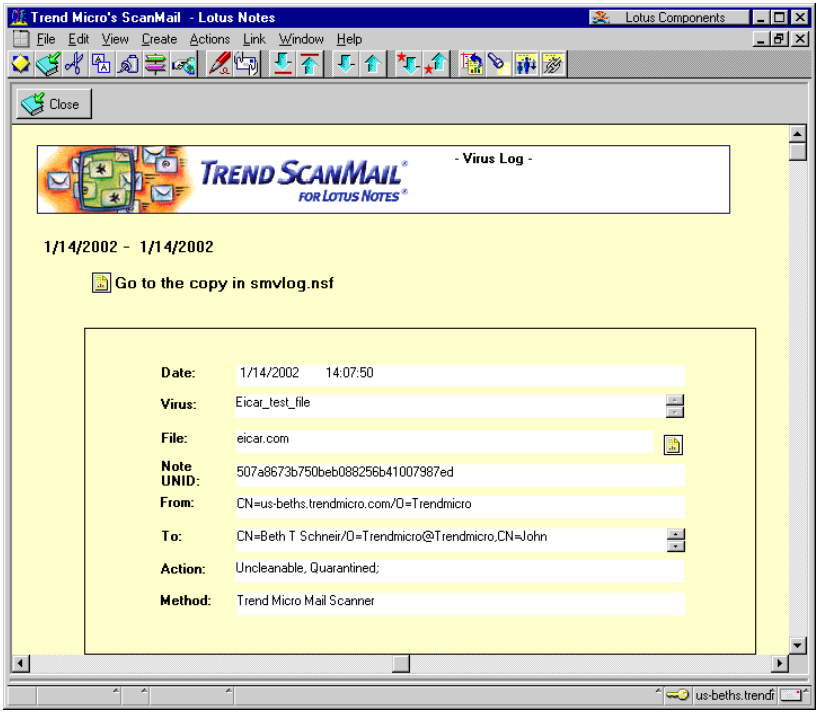


FIGURE 8-2. A detailed view of an individual record from the Virus Log.

3. Each Virus Log contains the following details:

- **Date** and time
- **Virus name** (or file blocked, hotspot name, or script name)
- **File name** the action was performed on
- **Note UNID** — the unique ID number of the document
- **From** and **To** (Email), indicating the sender and recipient of the email, or **From** (Database), indicating the database the document is located in
- **Action** performed on the file
- **Method** indicates which of the ScanMail scanners detected the virus, file, or script — email, database, or replication

4. If you configured saving a copy of the infected document in the virus log, you can click on the document icon at the top of the screen to go to the original copy in the Quarantine database.
5. To disable deletion of a selected file, click the **Disable Log Deletion** button in the Action Bar at the top of the screen. A "lock" icon appears to the left of the file name.

   If you later decide to delete the file, just click the **Enable Log Deletion** button to clear the lock on the file, then you can delete it by pressing the "Delete" key.

Note: The virus log files are automatically enabled for deletion by default. If you do not wish a log to be available for deletion, you must select it and click the **Disable Log Deletion** button.

---

6. You can display ScanMail's virus logs using one of several different views. To view the document details while still on the main log screen, click **View**>**Document**>**Preview**>**Show Preview** from the Notes menu**.** To configure the way the navigation window displays all three levels of information on the same screen, click **View**>**Document Preview**>**Arrange Preview**.
7. All aspects of the log files are presented in a single window, as shown in the previous figure.

Deleting log files automatically

ScanMail for Lotus Notes generates a log (stored as a new document in the smquar.nsf database) every time it discovers a virus. Depending on the volume of

traffic your machine handles and the number of viruses encountered, the log database may grow quite large.

Rather than always having to remember to manually delete log files, you can schedule the task to occur automatically. To do so, you need to add the ScanMail administrator's name to **Agent Restrictions**, under **Run *unrestricted* LotusScript/Java agents**.

To Setup Agent Restrictions:

1. From the main Notes admin console, open the Address book and then go to **Server > Servers** and select the name of the ScanMail server.
2. Click **Edit Server** in the Notes Action bar, and select the **Security** tab.
3. Scroll down the window that appears to **Agent Restrictions** and enter the name of the ScanMail administrator under **Run** *unrestricted* **LotusScript/Java agents**.
4. Click **Save & Close**, and return to the ScanMail console.

To automatically delete log files:

1. In the ScanMail menu, click **Logs > Log Maintenance > Scheduled Deletion**. The **Set Auto Delete Logs** screen appears.

2. Choose **Delete log files after {__} days**, specify a time interval, and click **Save & Exit** in the Action bar to complete the task.

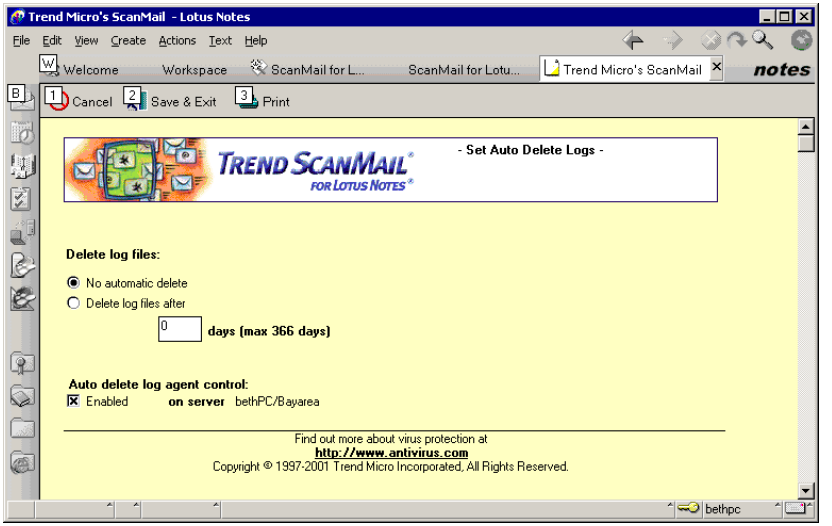


FIGURE 8-3. Scheduled Log Deletion configuration screen with the Auto Delete Log Agent Control enabled, but deletion of logs currently disabled.

Deleting logs manually

Before deleting a number of logs, it is a good idea to review them to be sure that they are indeed expendable. To perform a deletion, do the following steps.

To delete logs manually:

1. Select **Log Maintenance** to go to the log navigator screen**.**

2. Select **Manual Deletion**. The Manual Log Deletion screen appears as shown in the figure below.

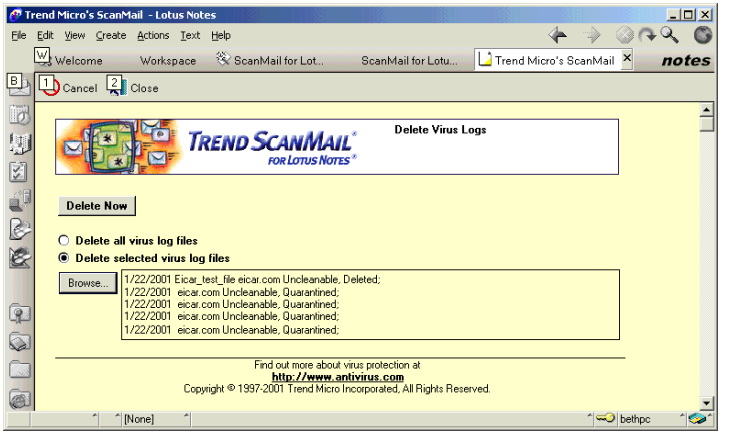


FIGURE 8-4. Manual Log Deletion screen

3. The following two choices appear:
   - To empty the log file database of all documents, click the **Delete all virus log files** radio button.
   - To select individual logs from a list of all the virus logs on the machine, click the **Delete selected virus log files** radio button. Click the **Browse** button that appears to produce a list of existing logs. Select the individual logs you want deleted and click **OK**. Return to the **Delete Virus Logs** screen to see a list of the files selected for deletion.

Note: If you have a large number of virus logs, we recommend that you select **Delete selected virus log files** to reduce the load on the server.

---

4. Click **Delete Now** to permanently erase the logs.

Using the Quarantine Manager

ScanMail automatically moves infected, blocked (eManager violations), encrypted, password-protected, and other designated message types to the quarantine database: `notes\domino\data\smquar.nsf`.

To view the quarantine logs:

1. In the main ScanMail menu, click **Quarantine Manager > View documents > [Infected Documents | Encrypted Documents | Blocked eMails | Blocked Attachments]**
2. Choose the time period for which you want to view the logs. You can display ScanMail's quarantine logs using one of several different views:
   - To view the document details while still on the main log screen, click **View | Document Preview | Show Preview** from the Notes menu**.**
   - To configure the way the navigation window displays all three levels of information on the same screen, click **View | Document Preview | Arrange Preview**. All aspects of the log files are presented in a single window.
3. To disable deletion of a selected file, click the **Disable Log Deletion** button in the Action Bar at the top of the screen. A lock icon will appear to the left of the file name.

   If you later decide to delete the file, return to the log and click the **Enable Log Deletion** button to clear the lock on the file, then you can delete it by pressing the "Delete" key.

Note: The quarantine log files are automatically enabled for deletion by default. If you do not wish a log to be available for deletion, you must select it and click the **Disable Log Deletion** button.

Setting virus log replication Connections

ScanMail provides you with the ability to automatically replicate the virus logs it generates using Notes native Server Connection functionality. Trend recommends that you set up *Pull Only* replications *to* the central Server *from* the peripheral servers (avoid Push-Pull).

To set a virus log replication connection:

1. From the Notes server where you want your aggregate virus logs to be kept, open the **ScanMail** console and then in the main menu, click Next, click **Log Maintenance > Log Replication**. The Notes Server Connection screen appears.
2. Click **Add Connection** to create a new replication connection.

Tip: You need at least Author rights to the Name and Address book to add the connection.

---

   a. Assuming that all the Notes-specific information is correct, enter the hierarchical name of the peripheral server(s) where ScanMail is installed in the **Destination server** field.

   b. Under Routing and Replication, enter **Replication** in the text field to the right of **Tasks**.

   c. Type ***Pull only*** in the text field to the right of **Replication Type**.

   d. Type the directory and database name of the log file, **`smquar.nsf`** in the text field to the right of **Files/Directories to Replicate**.

   e. Change the Routing Task field from Mail-Routing to **None**.

   f. Under Schedule, set the time interval and days you want to replicate the Quarantine database.

   g. Click **Save and Close** at the top of the window to create a connection document in the Server Name and Address Book.

3. Click **Esc** to return to the Log Maintenance screen.

Getting a statistical overview of virus activity

The Statistics option provides the ability to generate a numerical summary of the email and database virus logs on the server. It includes the aggregate number of viruses cleaned, deleted, quarantined and passed. It also includes new options to generate email statistics. To view virus statistics:

- Under the **Statistics** bar in the left navigator pane, you have five options:
  - Virus Charting

- Database Charting
- User Charting
- Virus Log Statistics
- Database History

Tip: If you do not have any virus logs currently, no data will be available.

Note: To display the charts, **Enable Java applet** must be enabled in Notes User Preference.

Virus Charting

Virus Charting provides you with reports of the top 10 viruses detected.

- Select **Virus Charting** and a pie chart appears with the top 10 viruses. If you have had fewer than 10 viruses, then there will be fewer "pieces" of the pie.

Database Charting

Database Charting provides you with information on the top 10 databases infected.

- Select **Database Charting** and a pie chart appears with the top 10 databases containing the most documents with viruses.

User Charting

User Charting provides you with information on the users who sent the most viruses via email.

- Select **User Charting** and a pie chart appears with the top 10 users who have sent the most viruses.

Virus Log Statistics

The Virus Log Statistics screen provides you with reports of virus activity over time. It includes the aggregate number of viruses cleaned, deleted, quarantined, and passed. In addition, the total number of files not scanned due to encryption is also available.

The Virus Log Statistics screen also reports the number of file attachments blocked and the number of destructive Stored Form hot spots and Rich Text hot spots found.

In a Notes server environment—where multiple instances of ScanMail are installed on server(s) and clients—the Virus Log Statistics screen can display the cumulative number of virus events encountered across the Notes network.

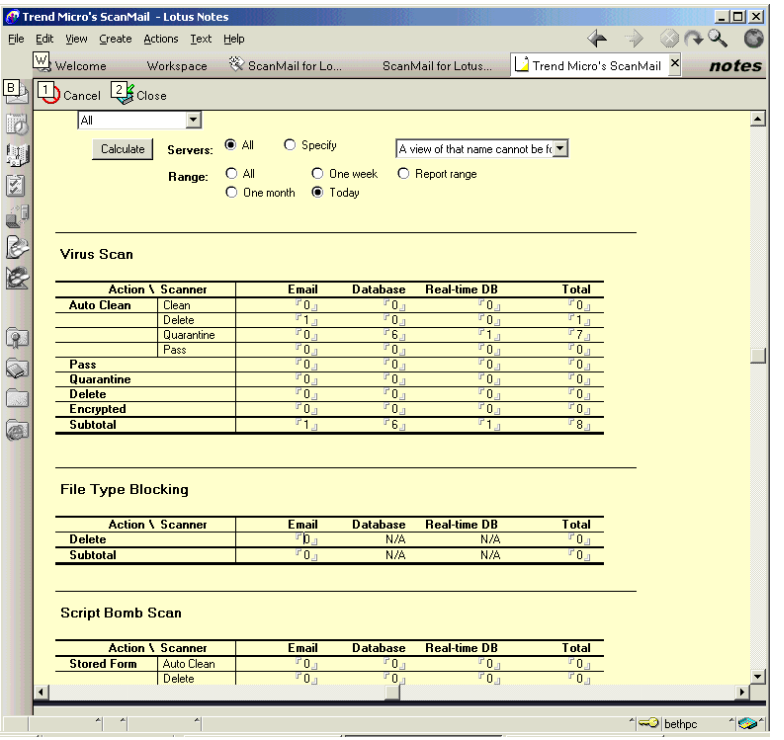


FIGURE 8-5. Virus Log Statistics screen presents an aggregate view of virus events.

To view virus log statistics:

1. Select the type of statistics that you want to generate. By default, **ALL** is selected and all 3 of the reports are generated. Alternatively, you can choose to generate just the **Virus Scan**, **File Type Blocking**, or **Script Bomb Scan** reports.
2. Choose the servers that you want the report to represent—**All** or **Specify** (and select a server using the drop-down arrow).
3. Choose the time period that you want the report to represent. You can select **One Week**, **One Month**, **All Dates**, **Today**, or a **Report Range**. If you choose **Report Range**, specify the range of dates using the drop-down month and date selections that appear.
4. Click **Calculate** to generate the report.
5. The Virus Log Statistics report shows Action rows by Scanner columns.

Virus Scan

The Virus Scan report shows actions on viruses classified under the statuses **Auto Clean**, **Pass**, **Quarantine**, and **Delete**. Within the Auto Clean category, there are also subcategories for files that could not be cleaned (Delete, Quarantine, Pass), as well as those that *were* cleaned. Encrypted documents are counted, but cannot be scanned on the server. The total number of files with viruses plus encrypted files is shown in the **subtotal** field.

Attachment Blocking

The Attachment Blocking report shows files deleted by scanner type.

Script Bomb Scan

The Script Bomb Scan report shows the actions of **Clean**, **Pass**, and **Delete** performed on Stored Form Script bombs. In addition, the actions **AutoClean**, and **Pass** are displayed for Rich Text Script bombs. The total number of Stored Form and Rich Text script bombs is shown in the **subtotal** field.

Total

At the bottom of the screen, totals are listed for all problematic files (Total = viruses found + encrypted documents + files blocked + files containing script bombs). The

report shows how ScanMail protects against viruses and script bombs, as well as blocks certain file types from entering the Notes network.

Database History

Select **Statistics**, then **Database History** to get to the history screen.

The Database History screen provides you with information about the scanning status of databases. You can find the date the databases were last scanned and the number of documents scanned in each database.

In addition, you can reset the Incremental Scan flag for a database. Just select the documents you want to rescan and select **Reset date to rescan all docs**. All documents selected are marked with the "Last Scanned" date of 01/01/0001, indicating that they have not been scanned for Incremental Scanning purposes.

Tip: Use this option, for example, when you have updated to a new pattern file and want to rescan all your existing databases for a new virus type.

Go to **Edit**>**Select All** and click **Reset date to rescan all docs**. All of your documents can then be rescanned with the new pattern file when you run a new Manual or Scheduled Scan.

System log

The Notes system log records information about all types of Domino server activities and remote workstation communication activities. System administrators should view it often to see whether databases are replicating properly, and to check for sufficient disk space and memory.

The system log includes the following fields:

- Database Size and Usage
- Mail Routing Events
- Miscellaneous Events
- NNTP Events
- Object Store Usage
- Passthru Connections
- Phone Calls
- Replication Events
- Sample Billing
- Usage

To view the System Log:

- On the main ScanMail menu, click **System Log**.

  ScanMail includes a variable called SMOutputLevel L in the Notes.ini file that you can set for different logging levels. This file is typically under `c:\winnt` for Notes R4 and `c:\lotus\domino\data` for Domino R5.

  - **Level 1** records virus information messages in the virus logs and the Notes system log.
  - **Level 2** includes Level 1 plus information about the activity of the ScanMail tasks, such as which databases were scanned.
  - **Level 3** includes Levels 1 & 2, plus more detailed logging information.

  Note: The ScanMail logging level is set by default at Level 2. You can edit this value in the Notes.ini file.

Chapter 9

Getting Help and Additional Information

Your copy of ScanMail includes an extensive online help database called `smhelp.nsf`, which is a native Notes database. Online help includes all the major topics included in this manual, from installation to advanced configuration. In addition, the **How to** section contains instructions on tasks commonly performed in ScanMail. ScanMail's Help database contains an FAQ section, which contains some of the most frequently asked questions about ScanMail for Lotus Notes. For the most up-to-date FAQ list, visit Trend Micro's Web site.

Trend Micro's Web site also has a wealth of information on the latest security threats, such as offensive email that can interfere with your companies' productivity. Visit Trend Micro's Virus Information Center to find information on viruses and malicious code threats. Visit "SolutionBank" for the most up-to-date error messages. SolutionBank is Trend Micro's free online database of common answers to technical questions.

Contacting technical support

Trend Micro can be reached via telephone, fax, email, regular mail, or through our Web page.

To find the contact information for the Trend Micro office nearest you:

- Open a Web browser to the following URL:
  `http://www.trendmicro.com/en/about/contact/us.htm`
- Alternatively, in the main ScanMail menu, click **Help > Support** or **Help > Help Database** to search for written information.

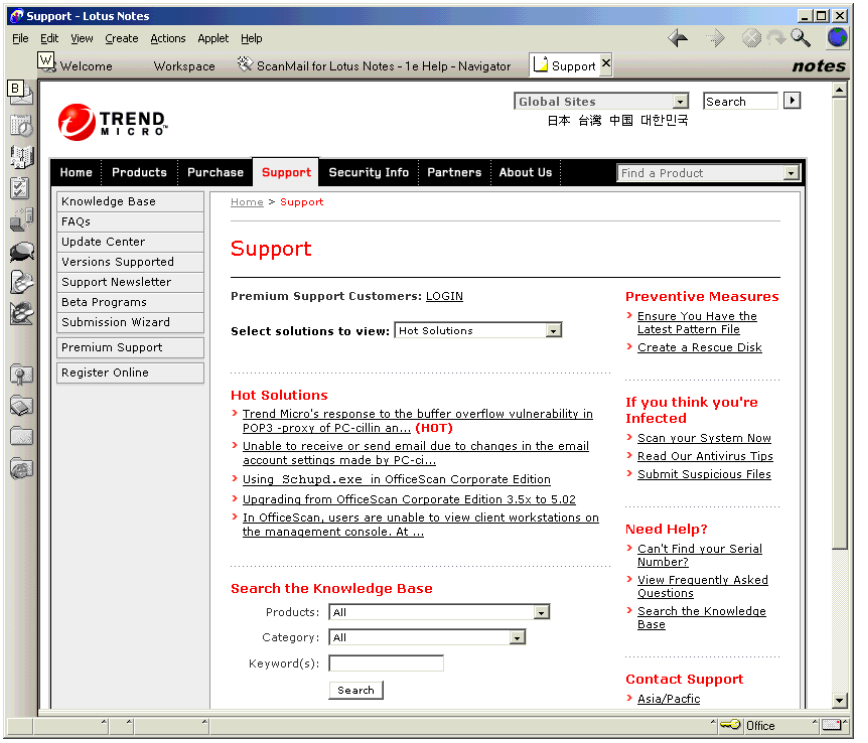


FIGURE 9-1. Access the Trend Micro Support page.

Speeding up your support call

To speed up your support call, have the following information available:

- ScanMail product, Virus Pattern File, and Scan Engine versions
- Operating system version and service pack version
- Lotus Notes or Domino release number
- Computer brand, model, and any additional hardware connected to your machine
- Amount of memory and free hard disk space on your machine
- notes.ini settings
- Exact text of any error message produced
- Steps to reproduce the problem

Program Status

To view a snapshot of ScanMail:

- From the main ScanMail menu, click **General Administration** > **Program Status** and then select the ScanMail server you want to the status of:
  - Scan status for real-time and mail scanners

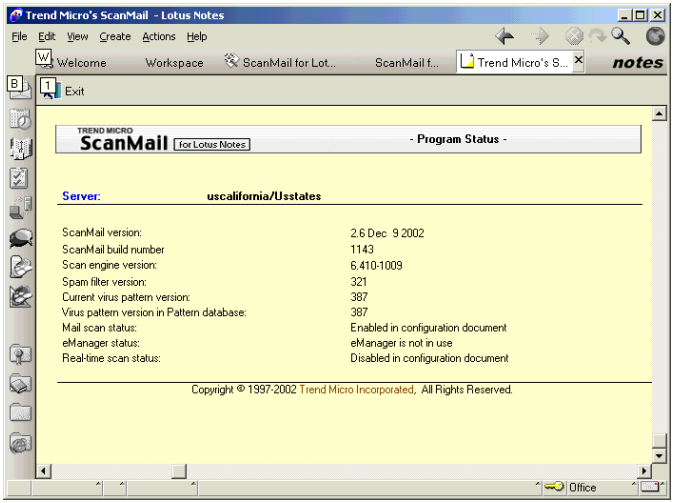


Figure 9-2. View a summary of all the critical information.

- ScanMail program version and build number
- Current engine version
- Current virus pattern file
- eManager status

Note: The virus pattern file may be a different version in the pattern database, `smency.nsf`, than the one that is currently being used for scanning.

Accessing the ScanMail online help database

The ScanMail Help database contains information on all the ScanMail features and provides cross-reference links to related topics. In addition, the **How to** section provides step-by-step solutions to common configuration questions. Consult this list first when looking for information on how to perform an operation in ScanMail.

Additional resources available over the Internet

The Trend Micro Virus Information Center provides many features to access virus information and security alerts. Visit HouseCall for a virus check-up. If you want to have regular virus alerts sent to you via email, sign up here.

Comprehensive security information is available over the Internet at our antivirus center

`http://www.trendmicro.com/vinfo`

Use the Virus Information Center to find out about:

- Which viruses and malicious mobile code are currently "in the wild," or active and a list of computer virus trigger dates
- Computer virus hoaxes and how to determine whether a detection is actually a false alarm
- Trend Micro’s Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- A safe computing guide

- Product details and white papers

In addition, you can sign up to receive

- A weekly virus alert, listing the virus outbreaks that occurred during the current week

Technical support knowledge base

If you receive an error message, or cannot find the answer to a given question in the on-line help, check the Trend Micro SolutionBank, an online knowledgebase filled with answers to technical product questions.

Use SolutionBank, for example, if you are getting an error message and want to search for any possibly solutions.

`http://solutionbank.trendmicro.com/solutions/solutionSearch.asp`

New solutions are added daily. However, if you don't find the answer you seek, you can submit your question on-line, where the personnel at TrendLabs will provide you with an answer or contact you for more information.

Using the Virus Encyclopedia

Trend Micro maintains a comprehensive Virus Encyclopedia with detailed information on tens of thousands of viruses. Virus descriptions include information on how the virus spreads, what kind of damage it can cause, how best to prevent damage, and how to clean up after being attacked by a virus (or Trojan, Joke, malicious applet, or any such "malware").

To open the Virus Encyclopedia:

1. From the main ScanMail menu, click **Help > Security Info** to open the Security Info Web page, and then **Virus Encyclopedia** in the Web menu that appears on the left.

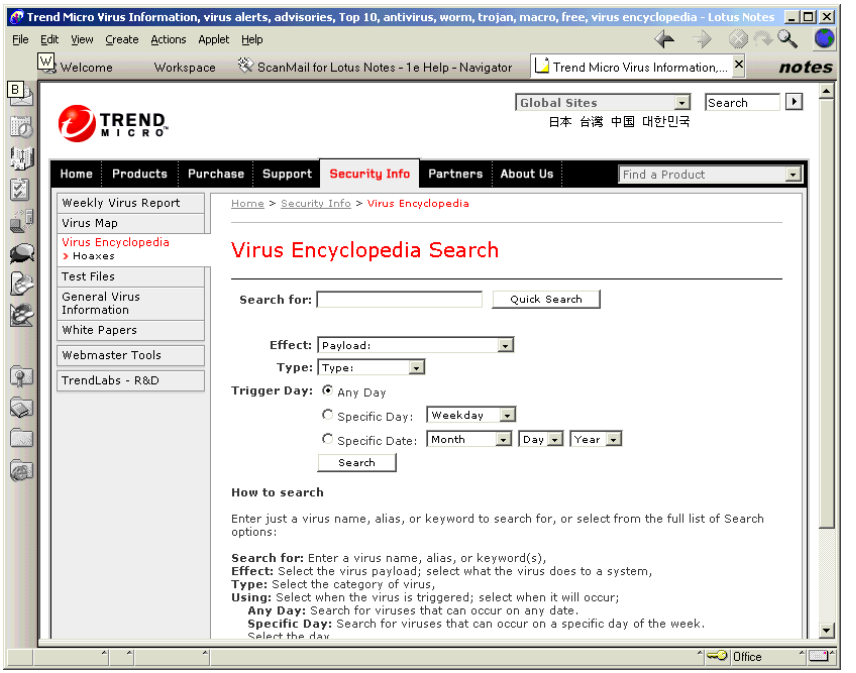


FIGURE 9-3. Trend Micro maintains a comprehensive virus encyclopedia.

2. To begin a search, enter a virus name, alias, or keyword. Otherwise, select from the full list of Search options:
   - **Search for**—Enter a virus name, alias, or keyword(s)
   - **Effect**—Select the virus payload; select what the virus does to a system
   - **Type**—Select the category of virus
   - **Using**—Select when the virus is triggered; or select when it will occur:
     - **Any Day**—Search for viruses that can occur on any date
     - **Specific Day**—Search for viruses that occur on a particular day

- **Specific Date**—Search for viruses that can occur on a specific date
- **Select**—the month, day, and year

TrendLabs™

TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world. (These centers are called "global antivirus eDoctor centers" in Japan and other Asian markets).

Staffed by a team of more than 250 engineers and skilled support personnel, TrendLabs' dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

Sending your infected files to Trend Micro

You can send your viruses to Trend Micro via the Web. More specifically, if you have a file that you think is infected with a virus but our scan engine does not detect it or cannot clean it, we encourage you to submit the suspicious file to us at the following Web address:

```
http://subwiz.trendmicro.com
```

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any virus(es) it may contain and return the cleaned file to you—usually within 48 hours.

Spam contact info

You can forward spam messages to Trend Micro at the following address:

```
spam@trendmicro.com
```

Spam received at this address is included in the anti-spam data file used by eManager.

Chapter 10

Control Manager Agent for ScanMail

In addition to the local console, ScanMail can be administered through the Trend Micro Control Manager (TMCM), a centralized system that unites your Trend Micro antivirus products into a cohesive virus security and content management solution

Through Control Manager, multiple instances of a product can be grouped together and administered as one.

FIGURE 10-1. Viewing ScanMail program status from Control Manager.

Virus logs can be aggregated from your entire network and analyzed to provide a comprehensive picture of virus and other activity on the network. ScanMail can be administered in context with the rest of your antivirus products installed on the network.

Running ScanMail in a Control Manager environment also brings to it a framework for the Outbreak Prevention Service, Trend Micro's unique protection service designed to keep connected enterprises informed and protected against virus and content threats. See *About Outbreak Prevention Service* on page 10-5.

The Trend Micro Control Manager agent for ScanMail is optionally available and can be separately obtained by contacting your Trend Micro representative.

Note: You cannot use a Trend Virus Control System (Trend VCS) agent to connect ScanMail to the Control Manager server. Control Manager does not support multiple, simultaneous program updates for ScanMail

---

To bring ScanMail into a Trend Micro Control Manager network, start by installing a Trend Micro Control Manager agent to each ScanMail server. (Later, you can aggregate individual instances of ScanMail into a single "virtual product" in the Control Manager directory tree).

Control Manager Features

Control Manager builds on the centralized management concept Trend Micro pioneered with Trend VCS. Trend VCS is the previous name for what is now known as Control Manager. If you are currently running Trend VCS, you can purchase an upgrade to obtain all the new benefits of Control Manager. For more information on upgrading your management server from Trend VCS to Control Manager, see the Trend Micro Control Manager Getting Started Guide.

Key features include:

Proactive Outbreak Prevention—With Outbreak Commander, you can take proactive steps to secure your network against an emerging virus outbreak. Outbreak Commander provides a proactive attack protection service. It blocks malicious code, by file name or specific file details, while new pattern files are being developed that can detect and clean the new threat.

- **Secure Communication Infrastructure**—Control Manager uses a new, communications infrastructure—built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, transmissions can be encrypted, or encrypted with authentication.
- **Task Delegation**—Each user can be given a personalized account with their own privileges, which defines what the user can see and do. Account usage can be tracked via user logs.
- **Command Tracking**—This feature allows you to monitor all commands executed on Control Manager. This is particularly useful for determining whether or not long-duration commands—like virus pattern updates for example—were performed successfully.
- **Real-time Product Control**—Control Manager provides you with real-time product control. Configuration changes made on the console are immediately sent to the products; even manual scans can be run from the console. This latency-free command system is indispensable during a virus outbreak.
- **Centralized Update Control**—Centralized updates of your anti-spam rules, and virus pattern and scan engine files ensure that all products contain the latest components. It also makes it possible to view your entire network's protection status from a single management console.
- **Centralized Configuration**—Centralized configuration allows you to coordinate virus-response and security efforts from a single console to ensure consistent enforcement of your company's virus and security policies.
- **Centralized Log Reporting**—Get an overview of your antivirus and content security network's performance using comprehensive logs. Control Manager can collect logs from all its managed products; you no longer need to check the logs of each individual product.
- **Centralized Management**—Allows administrators to configure, monitor, and maintain most Trend Micro software installed on the network from a single console regardless of location or platform.
- **Flexible and Scalable Configuration**—Simplifies the administration of a corporate virus and content security policy.
- **Insulated Administration**—Allows you to compartmentalize Control Manager administration rights and product views according to a variety of criteria. For example, you may wish to have certain administrators only see certain products.

You can use Control Manager to unify the administration of multiple instances of ScanMail on the network:

- Configure groups of ScanMail servers as if they were one
- Update virus pattern file and scan engine
- Aggregate virus logs from multiple ScanMail servers
- Aggregate virus activity detected by ScanMail with records from other protection points on the network (such as at the Internet gateway, the file server, or each individual desktop).

About Control Manager

The Trend Micro Control Manager, (previously called Trend Virus Control System, or Trend VCS) is a centralized management console for coordinating, tracking, and maintaining the variety of antivirus software products that are often found installed on a LAN or WAN.

Because Control Manager allows a single administrator to unify and manage all the different antivirus products on the network—regardless of platform or physical location—it is an especially useful tool for large, dispersed, and complex networks.

For example, from the Control Manager console you can configure all antivirus programs on the network to behave in the same manner, view aggregate virus logs for virus events WAN-wide, and update the Virus Pattern files for all programs.

How Control Manager works

The Control Manager server communicates with each managed product using an agent, a small program that enables communication between Control Manager and the product.

If you have a widely dispersed network with multiple instances of ScanMail, Control Manager greatly reduces the time you spend configuring your servers, as well as increases your network visibility.

Control Manager uses the Secure Socket Layer (SSL) protocol and communication between the Control Manager server and managed product(s) supports both encryption and authentication.

About the Communicator

The agent package is composed of two parts, the Communicator and an agent.

The Communicator is the managed product-side component of the Trend Micro Management Infrastructure (TMI) — the communications backbone of the Control Manager network. Control Manager agents have their own local Communicator, which is shared by all the agents on that server. Though there can be as many agents on a server as there are managed products, only one Communicator is required for each server. The TMI uses the same encryption key and message routing settings for all agents installed on a server.

Agents typically receive data from the Control Manager server and configure it to fit the requirements of the managed product. Likewise, they collect log data from the product, and reconfigure it to the requirements of Control Manager.

About Outbreak Prevention Service

The Outbreak Prevention Service (OPS) allows enterprises to take proactive steps against new virus threats before the necessary virus pattern file update becomes available. By bridging the gap between threat notification and virus pattern delivery, enterprises can quickly contain virus outbreaks, minimize system damage, and prevent downtime.

OPS provides you with outbreak prevention policies product setting recommendations designed to secure your network during outbreaks. These policies are applied to the products managed by Control Manager using Outbreak Commander.

Outbreak Commander applies policies in the following stages:

- **Prevention**—threat information delivery and deployment of precautionary content security policies while a new virus pattern file is being developed.
- **Notification**—notifications are automatically sent to the individuals and groups configured.
- **Scanning**—real-time scanning on antivirus products is enabled
- **Updates**—a new virus pattern file is deployed to the antivirus product. If the threat requires development of a new scan engine, the scan engine can be automatically deployed as well.

System requirements

To install the Control Manager agent for ScanMail, you need the following hardware and software:

- Microsoft Windows 2000 Server or Advanced Server; or Microsoft Windows NT 4 with Service Pack 3
- Intel™ Pentium™ 300MHz processor (or higher recommended)
- 128MB RAM minimum (256MB or more recommended)
- 50MB free disk space for the agent program files

Note: The Control Manager agent must be installed on a NTFS partition, and installed while logged on using Windows administrator-level credentials with Domain Administrator privileges.

Using Control Manager to Unify ScanMail Management

If you are running more than one instance of ScanMail on the network, you can make uniform configuration changes, analyze virus logs, and make simultaneous virus pattern and scan engine updates if you "attached" the ScanMail to Control Manager by installing an agent.

Notes:

- Install one agent on each server running ScanMail
- Only servers of the same platform can be updated simultaneously
- If there is already a TMCM agent on a given server, for example because another antivirus product is installed on the same server, you should still install the agent for ScanMail
- For Domino partitioned servers, install a separate instance of the agent on each partition
- Since the agent Setup requires the Domino server to be running, but the ScanMail Setup requires the Domino server to be stopped, you should install ScanMail on all your partitions first, start the server, and then install all the agents

Installation planning

Although agent installation is pretty straightforward, prior to running Setup there are two things to plan for to ensure a successful installation:

a. Gather relative network information

b. Obtain a Control Manager public key

A. Gathering relative network information

Before installing the Control Manager agent, know the following:

- The Fully Qualified Domain Name (FQDN) or IP address of the Control Manager server to which the agent will report
- Windows Administrator account credentials for the agent server
- At least one shared drive on the agent server

- A Control Manager User ID with an Administrator, Power User, or Operator account type

Additional installation notes:

- Do not delete the Windows account used to install the Control Manager agent or it will not be able to re-register with the Control Manager server
- Control Manager agents cannot be installed using Terminal Services
- A Control Manager 2.5 agent should only be installed to a Control Manger 2.5 network (do not install to a Control Manger 2.x or Trend VCS managed network)
- Even if you have installed a Control Manger agent for ScanMail on a given machine, it is still necessary to install an agent for ScanMail

B. Obtain a Control Manager public encryption key

Before running the agent Setup program, obtain a public key and copy it to a known location on the ScanMail server.

To obtain a Control Manager public encryption key:

1. Open the Control Manager console at:

   `http://computer name/ControlManager`

   where “computer name” is the IP address or host name of the Control Manager server.
2. Enter a **User ID** and **Password**. The User ID can be a Control Manager Operator, Power User, Administrator, or Root credential.
3. Select **Products** > **Add/Remove Product Agents** and right-click the **public encryption key**. Save the file (named `E2EPublic.dat`) to a location accessible to the server where agent will be installed.

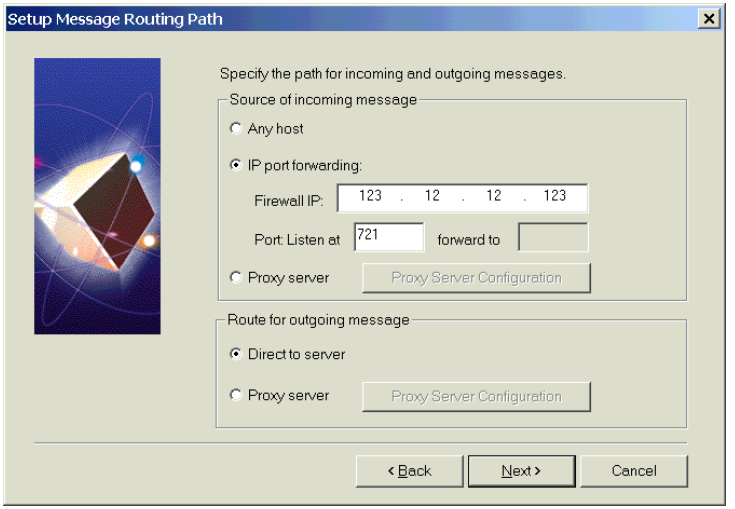
Installing the Control Manager agent

The Control Manager agent for ScanMail provides a communication link between ScanMail and the Control Manager console.

Install one agent on each ScanMail server. For partitioned servers, install one instance of the agent on each partition. Since ScanMail must be installed with the Domino server shut down, and the agent with it running, install all instances of ScanMail first, before re-starting the server and running the Agent installs.

To install the Control Manager agent:

1. Locate and then run the program agent Setup program, typically in the `\cmagent` subdirectory of the ScanMail installation directory, or, if you have the Enterprise Protection CD, in the `\products\smln\cmagent` directory on Disk 1.
2. In the Welcome screen that appears, click **Next**, and then **Yes** to accept the License Agreement. The Setup Message Routing Path screen appears.



3. Next, specify how you want inbound and outbound messages (virus notifications, for example) routed and then click **Next**. Choose:
   - **Any host**—to have agent will accept messages sent to its port from any source. This is the least secure

- **IP port forwarding**—if the Control Manager server will be receiving message traffic from a 3rd-party such as a firewall. Specify the IP address and port where Control Manager should listen for inbound traffic.
- **Proxy server**—if there is a proxy server between the agent and Control Manager server. Click **Proxy Server Configuration** and then type the IP address or host name, port, and any log in credentials.

Route for outgoing message

- **Direct to server**—to have the agent contact the Control Manager server directly. This is the least secure.
- Proxy server—(as above) if there is a proxy server between the agent and Control Manager server.

4. In the Register with Control Manager screen that appears, click **Import** and then locate the Control Manager public key you generated (typically, this file name is `E2EPublic.dat`). Click **Next** to continue. Setup will take a moment to copy files and install the TMI (a part of Control Manager-agent relationship).

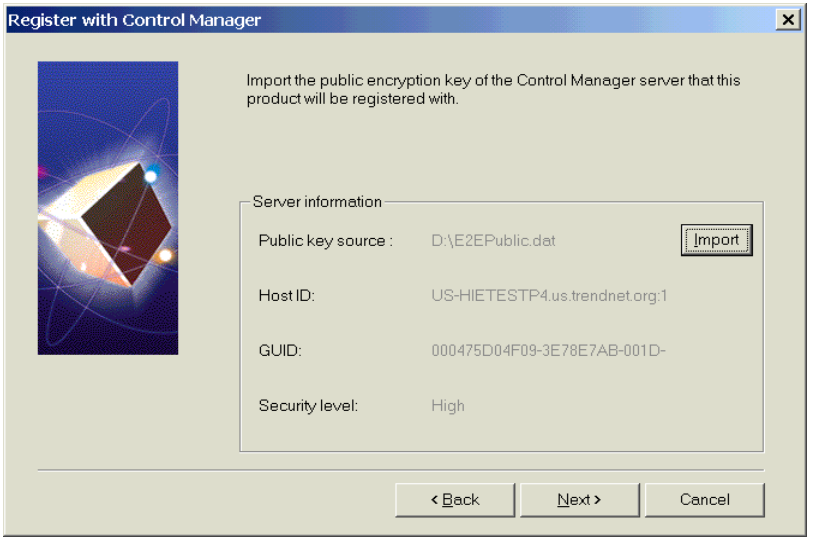


FIGURE 10-2. The agent will contact the Host ID.

Tip: You can ping the server to be sure both the host name and fully qualified domain name are recognized (if the ping fails, edit the file: \winnt\system32\drivers\etc\host on the agent server to associate the hostname, FQDN, and IP address)

5. In the Select Notes.ini screen, identify the location of your notes.ini file and click **Next** to continue.
6. Finally, enter root-level login credentials to the Control Manager console, typically "root" or "administrator", and specify the group name you want this agent to appear under in the Control Manager product tree:

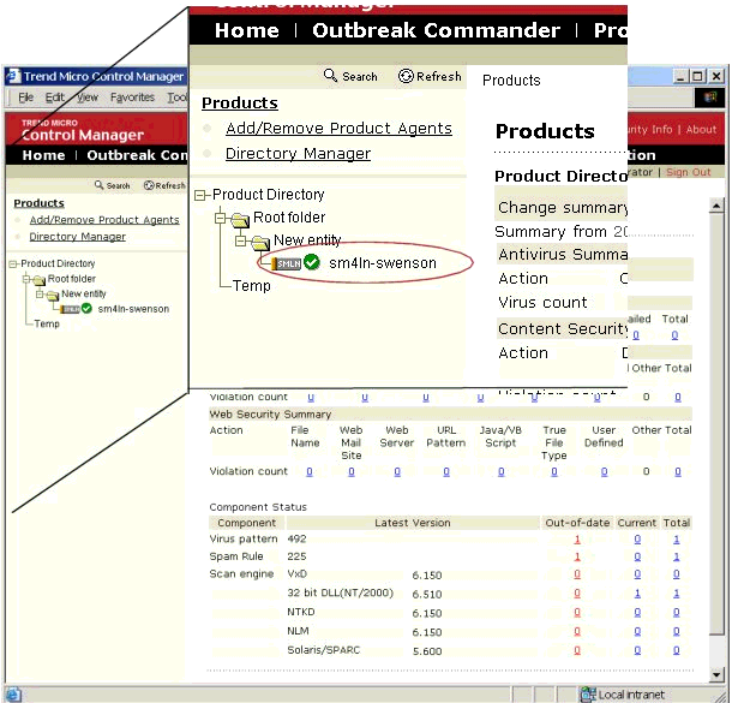


FIGURE 10-3. The Entity name you choose when installing the agent will appear in the Product Directory in the Control Manager console.

Opening the Control Manager console

ScanMail can be securely administered via Control Manger from the ScanMail server, or from any computer on the network. The Notes **HTTP** task must be running on the Notes server where the ScanMail agent is installed in order to access the agent from the Control Manager browser.

To open the Control Manager console:

1. From the ScanMail server or any other computer on the network, open a Web browser and then enter the URL of the Control Manager server, for example:

   ```
   http://IP address/ControlManager
   ```

2. When prompted to type in a Control Manager User ID and password, use the credentials you used when installing the agent. (If you use a different account, ScanMail may not be visible in the Control Manager product tree—only root-level accounts can view all products in the tree).
3. When the Control Manager console opens, click **Products** in the menu bar, and in the product tree that appears on the left, click **Product Directory**>**Root folder**>**New entity** and choose the instance of ScanMail that you want to view or manage.

Using Control Manager

From the Control Manager console, you can view a summary report of ScanMail, make specific configuration changes, deploy new spam rule files to the ScanMail server, and analyze activity by viewing the ScanMail log files.

In addition, you can manage your entire antivirus network, including running the Outbreak Commander. For complete Control Manager information and instructions, see the Control Manager on-line help.

Reading Status Reports

The Status Report for ScanMail provides key product details for any given installation, including product version and build, current spam rule, time of last update, etc.

To view the ScanMail Status Report:

1. With the Control Manager console open, select the ScanMail you want to explore from the **Product Directory**. The **Status** window appears.
2. Look through the report to find, for example, the following:

Product type	Version/Name
Product	**ScanMail for Lotus Notes**
Product version	2.6
Agent version	2.5.1101
Registered with Control Manager	2002/11/12
Status	Running since 2002/4/15
Spam rule version	n/a
Spam rule information	AntiSpam.549 (Updated 2002/11/11) Trend$SE.190 (Updated 2002/11/07)
Virus pattern version	n/a
Last Update Time	n/a
Scan engine version	n/a

Administering ScanMail from Control Manager

The Configuration screen allows you to make sequential configuration changes to all the ScanMail servers in the product tree.

Note: The HTTP task must be running to support this.

To open the ScanMail Configuration page:

1. With the Control Manager console open, select the ScanMail installation you want to view or manage from the **Product Directory** and click the **Configurations** tab.
2. Choose **ScanMail (ver)** from the product list that appears, and **Configure ScanMail**, then click the **Next** button. The ScanMail console appears.

3. Configure ScanMail as you would from the local interface.

Updating the spam rule

You can update the spam rule file for your ScanMail server or servers from the Control Manager console. Unlike for antivirus products, spam rule updates must be performed sequentially—they cannot be cascaded across a group.

To deploy a spam rule update:

1. With the Control Manager console open, select the ScanMail installation you want to explore from the **Product Directory** menu and click the **Tasks** tab.
2. Choose **Deploy virus pattern/spam rule** from the task list that appears, and **ScanMail (ver)** from Supported products. Click the **Next** button. The **Deploy now** window appears.
3. Click **Virus pattern / Spam rule** to begin updating the ScanMail server with the current spam rule from Trend Micro.

Monitoring security and event logs

ScanMail keeps detailed logs of all spam and content rule matches, system events, and other information. You can review the logs online, in real time, or you can export them to a comma separated values (CSV) file and use a third-party database or spreadsheet program to perform additional analysis and/or charting.

To view security and/or event logs:

1. With the Control Manager console open, select the ScanMail installation you want to view from the **Product Directory** menu and click **Logs**.
2. Choose the type of logs you want to view—Security or Event.

Note: Events specific to ScanMail appear only in the content security violations portion of the Security log.

- **Security logs**—includes all virus log incidents, *content security violations*, viruses found in download traffic (HTTP, FTP), email, files, and Web security violations

- Event logs—includes virus outbreaks, module updates, service on/off notifications, and security violations

3. After choosing the type of logs you want to view, either Security or Events, specify a time period, log type, sort order, etc. and run the query to view the results.
4. Click **Save Log as CSV** to export the on-screen data to a comma separated values file.

Note: Right-click the **Retrieve the File** link and select **Save target as** to copy the CSV file to the location of your choice, or left-click the link to display the data in the Control Manger Tasks window.

Group configurations

Using Control Manager, you can configure and perform tasks on multiple antivirus products at the same time (with ScanMail being one exception). Control Manager requires only that the same version be used when performing group configurations and that the servers are listed in the same Control Manager product folder.

To uniformly configure multiple servers:

1. In the Product Directory on the left-hand menu, navigate to the desired folder under which your ScanMail servers are listed.
2. Select the folder that contains the ScanMail servers.
3. Select a configuration tab in the main menu. The controls in the Status, Configuration, Tasks and Logs tabs will affect all servers in the folder that use the same version of ScanMail.

Getting additional help

For complete information on Control Manager and/or ScanMail, check the respective product's documentation set:

- **Getting Started Guide**—introduces the product, installation planning, installation, and configuration needed to get the product up and running
- **On-line help**—explains, in detail, individual features, fields, and tasks

- **Readme.txt**—contains late-breaking information and a record of incremental program enhancements and bug fixes
- **SolutionBank**—the Web-based Knowledge Base, contains known issues and specific-problem solving procedures

Removing the Control Manager agent for ScanMail

If you want to remove ScanMail, the Control Manager agent, or both, always start by removing the agent first, then the product, and finally, the TMI (Trend Micro Infrastructure). To remove the agent only, you do not have to remove the TMI.

To remove the Control Manager agent:

1. From the Windows taskbar, click **Start**, then **Settings > Control Panel > Add/Remove Programs**.
2. Scroll down the list to select **Trend Micro Control Manager Agent**, then click **Remove** and **Yes** to begin removing the Control Manager agent.
3. After Uninstall is complete, click **Close.**

Index

N

O

P

Q

R

S

T

U

V

W